Culture & Empire

Digital Revolution

Culture & Empire

Digital Revolution

Pieter Hintjens

For Sheila

Culture & Empire

Edition 1.3: 19 December 2013

Published by iMatix Global Services

Edited by Gillian McGarvey and Dr. Helen Hintjens

Cover by westinCovers, www.westincovers.com. Fonts: Kontrapunkt (Bo Linnemann, Kontrapunkt A/S), Existence (Yeah Noah), DJ Gross (SDFonts), EB Garamond (Georg Duffner)

ISBN 978-1492999775

Contents

Preface

Once upon a time, there was a great Empire that ruled the known world.

Cost Gravity: The Endless Fall to Free

For fifty years, Moore's Law has reliably predicted the exponential upward trend of our silicon future. Yet every now and then, technology tabloids warn that Moore's Law is about to end. It can't last, we're told, and when it ends, the future will fall into darkness and uncertainty. Yet inevitably and without fail, scientists find yet another way to extend it, and we collectively sigh in relief.

Moore's Law isn't a mythical beast that magically materialized in 1965 and threatens to unpredictably vanish at any moment. In fact, it's part of a broader ancient mechanism that has no intention of stopping. This mechanism, which I call *cost gravity*, pulls down the price of technology by about half every two years.

Cost gravity affects our entire human world. It is inevitable and unstoppable, driven by the spread of information and knowledge. Every two years, any given technology becomes twice as available at half the cost, and twice as powerful with half the bulk. Look around and observe that many old (and previously expensive and large) technologies are effectively free today, except for the influences of other ancient forces such as natural resources and friction. Cost gravity has existed and will exist as long as life itself.

Superficially, technology is a human invention. Broadly, however, *all* life is information-based and therefore subject to cost gravity. Take bacteria, for example. Bacteria are highly advanced life forms that evolve rapidly to survive in almost any condition. Bacteria share their genes in the way open source programmers share their code. Antibiotic resistance is scary, not because there's one colony of resistant bac-

teria somewhere, rather because these genes can pass to other bacteria that need them. Bacteria have recently been found in the inhospitably frozen Antarctic. Genetic information flows through the bacterial world just like knowledge flows through the human world.

Or consider a living cell, which has more moving parts than a Boeing 777 and is smaller than a micron. Cells are self-healing, self-reproducing, and self-organizing. You might be tempted to invoke the supernatural to explain such sophistication. The real answer is that cells represent three-and-a-half billion years of cost gravity at work.

In human society, cost gravity makes expensive technologies into cheap ones. The curves are exponential: price falls to zero, power rises to infinity. Cost gravity does more than explain why so many things are more affordable than ever before; it provides a context for human history. Cost gravity takes emperors' toys and turns them into commoners' tools, and as it does this, it drives profound social, economic, and political change.

Here's how it works: A vital new technology enters society as an expensive item for the wealthy elite. The elite use it to expand their power base. However it's the middle classes who actually make the products. The technology naturally falls into their hands and they aggressively improve it. They compete for customers by making it faster, cheaper, and more reliable. The technology enters mass production and becomes available to all. The farmer and the laborer suddenly gain access to this new power. Society reshapes itself like bubbles in a lava lamp. New businesses emerge and power moves from old to new.

Inevitably, old money fights back and tries to squash the newcomers. It buys oppressive laws, builds police states, and crushes the commercial middle classes. Old money sometimes wins, though not for very long. Political systems crash and are replaced by new ones. The page turns and the story starts again.

Most histories overlook this process and focus instead on political changes and events without explaining why they happen. I argue that every great empire is born out of a monopoly on a vital new techno-

logy: bronze, iron, the horse, irrigation, roads, military organization, finance. In each instance, essential knowledge spreads until everyone has access to it. Then the empire loses its monopoly, crashes, and the cycle repeats.

It is hard to understand exponential curves. Our minds give up as we approach the infinite. The curve tends to look either totally flat or like a straight cliff. We can look at history and collapse it into: "clean water and roads let the Romans build their empire" or "my portable phone has more computing power than the whole of NASA in 1962." When I tell you that in 60 years, the average person on the planet will have and use more computing power than the entire Internet today, does that concept fit into your world view?

One reason the phenomenon is hard to grasp is that there is not one single technology to consider, rather, millions. The key ones are those that solve critical problems yet remain too expensive for common use, such as solar power, genetic engineering, advanced medicine, privacy, high-bandwidth communications, higher education, political organization, insurance, banking, translation, and so on. It's fair to predict that all of these — at least when the patents, which I'll talk a lot about later in this book, have expired — are affected by cost gravity and will be one-thousandth the cost in 20 years, and one-millionth the cost in 40 years.

Once we realize that the curve has always existed and will always exist, we see that there is no coming "singularity." What does happen, predictably, is that as the cost of key technologies falls below certain thresholds, these technologies create explosive changes in society. While the curve is mostly invisible, these tipping points are not.

To take one historical example, paper existed for thousands of years, yet only in the fourteenth century did it become a mass-market product. There is a theory that the Black Death left enough cheap linen clothing lying around to spawn the mass production of paper. This is a possibility. More likely, the price of paper fell (thanks to cost gravity) below the critical level where any household could buy a printed

book. At any rate, cheap paper broke the church's monopoly on information and opened the way for the Renaissance.

In the last decade, we crossed another one of those tipping points as computing — once the key to global monopolies in finance and industry — dropped into the range of the average household budget. Our twentieth century empires are crashing, and we're witnessing that crash and the seeds of the rebirth.

What Happened to Wall Street?

In 2007, it was already clear that multiple bubbles (consumer credit, the housing market, the trade in derivatives, and so on) were going to burst sooner rather than later. In 2009, banks and entire countries started to collapse. Today, we are still picking up the pieces and the bill. Most of us were — and still are — surprised and shocked. The common view was that banks were invulnerable. After all, they were among the wealthiest institutions on the planet. They were literally "where the money was." How can a bank's share price go down? Later, as bank after bank failed and had to be rescued by the taxpayer, the general public was shocked. The only possible cause must have been corruption and fraud.

For sure, corruption and fraud were present. As Naomi Klein lucidly explained in her 2007 book "The Shock Doctrine"[1], any crisis is an opportunity for the mega-bandits to move in and empty the coffers. It's certain that some groups knew that banks would collapse and bet heavily on that. The crisis was long in the making. It was fully predictable; indeed, it was inevitable.

Here's why. Let's rewind 30 years and see how the banks work. We're in 1980, and banks are the shining cornerstones of modern society. They are large, boring houses for financial machines. The banks arbitrate between those who have money and those who need it, a vital service for which people gladly pay. Critically, this service takes vast amounts of computing power. Simply adding and subtracting and

1 http://www.naomiklein.org/shock-doctrine

multiplying and dividing all those figures takes industrial-strength brute force. Banks have huge data centers: rows of blinking mainframes and humming disk drives, all adding up to tons of heavy metal in massive air-conditioned halls.

Meanwhile — silent and unstoppable — the spread of knowledge drives down the cost of computers. First, smaller and cheaper minicomputers spread into departments. Then the personal computer explodes into the home, university, and business. Large firms like IBM try to keep their prices stable, meaning they give their customers more and more computing power for the same price.

The true cost of building a bank-sized data center drops by 50% every two years. The result is that older banks start to face competition from small aggressive competitors, especially as the Internet begins to make the local branches obsolete. The big banks grow by buying smaller local banks, an easy task due to the fact that they possess lots of excess capacity. Then, they cut costs by shutting branches and merge with insurance companies to expand their services.

All the while, competition is driving down profit margins. If your bank asked 5% per year for a mortgage and another bank 1,000 km away offered 4%, you would not hesitate to go with the lower rate. Similarly, if your bank offered 3% interest on savings, and a foreign competitor offered 6%, where would you put your money? For years, in Europe, you could literally earn 2-3% more on deposits than you had to pay on a mortgage. This should have been a clear sign of trouble, yet people just assumed there was some magic at play.

Fast-forward a few more years, and banks' main traditional markets are close to worthless. The European single market means they face ever more competition. They're in a trap, borrowing money from the stock markets in order to expand internationally so that they can compete. It's a one-way trip. If you don't make your quarterly profits, your stock price falls and your cost of borrowing rises. The only banks that escape are those who stick to luxury products for the richest clients and avoid the stock markets.

The large banks *must* find ways to continue to make their 6% profit annually. And higher profits come only from higher risks; there is no other route. So governments oblige by removing regulations, and banks get new high-risk space to move into. They push mortgages onto people who cannot afford them. They push credit cards so aggressively that even a dog can get one. And as they accumulate more and more risk, they hide it from view by repackaging it all into derivatives, which they sell to foreign banks. Eventually, the trade in derivatives becomes the new territory and banks turn into bookmakers, betting against themselves and taking a commission on each deal.

Meanwhile, cost gravity never stops. By 2013, the cost of running a 1980's bank had fallen by 128,000 times. If it cost $10 per month to handle one customer in 1980, by 2013 it cost just over $75 per month for 1M customers. And by 2052, it will cost only $1.00 per month to handle the banking needs of every person on Earth.

The collapse happened because those ever-riskier bets didn't pay off. It was predictable, and some people did predict it[2], yet there was a huge incentive for those involved to not think it through. You might feel as though it was criminally stupid to make those bets. Certainly, it was immoral to have the public purse pay the debt while still giving bonuses to all involved. In the end, every empire bets on borrowed time. It's always the same, whether the time scale is "next quarter" or "next century." Bank or beggar, life is always "so far, so good."

When we understand that cost gravity caused the banking crash, we can try to predict the future of banking. Banking is an essential service. However, it cannot be profitable except by rolling back time and banning cheap information technology, or by creating artificial barriers to competition.

There seem to be two plausible outcomes. One is to nationalize the large banks and turn banking and insurance into a not-for-profit service of the state. Europe seems to be going this way. As part of their rescue packages, many countries took control of failing banks like

2 http://www.eupaco.org/report:david-martin

ING, BNPParibasFortis, Dexia, and ABNAmro, and cleaned out the existing management. Whistle blowers have helped the new technocrat owners launch prosecutions for manipulation of share prices and other forms of fraud. Ironically, 20 years ago and before the trend of privatization, many of these banks were publicly owned state banks.

In the US, the trend is quite different. Instead of intervening in the running of the banks, the US government intervened in the markets. They helped the largest banks like JPMorgan Chase & Co. buy up their competitors at fire sale prices, keep their existing management with no investigations or prosecutions, and gain monopoly control over the market to extract profits as before. The US approach seems similar to how mobile phone operators have an effective cartel, with government support, to extort profits from phone and Internet users.

The Digital Revolution

When I started studying at the University of York, Computer Science wasn't yet a proper subject; it was an abstract (and mostly tedious) offshoot of mathematics. It was another 10 years before I got my first modem and connected to the embryonic Internet of email, news groups, and bulletin boards of the early 1990's.

We are close to full planetary connectivity[3] by at least mobile phone, and increasingly via smartphones that provide Internet access. Getting on line — even if "only" via a shared mobile phone — is the surest way to escape poverty, just as moving to a city was previously the best way to escape poverty since the nineteenth century.

Powered by steam and coal, the Industrial Revolution of the late eighteenth and early nineteenth century brought people into new cities where they redefined social, economic, and political reality. The new social concentrations of nineteenth century industrial cities allowed an entrepreneurial middle class to emerge, and quite rapidly their economic power turned into political power. In 1848, a political

3 https://www.google.com/search?q=how+many+phones+in+the+world

revolution occurred across Europe, leading to the establishment of parliamentary democracy in many countries.

The Digital Revolution is having the same effect: people congregate into new communities and entrepreneurs build new economies around those communities, which form a new economic class. When their economic power exceeds that of their old "legacy" competitors, and as the fights break out, they begin to seek political representation and power. Economic change leads to social change and then political change: all of it driven by cost gravity.

Technological revolutions express themselves as class struggles. The upper class is the "old money": those who were rich and powerful under the old system. The middle class is the "new money": those who have adapted to exploit new opportunities by breaking and redefining convention, and who are growing richer. The lower classes, unable to make the leap into the new social models, are excluded from the new prosperity. The true lower classes of the Industrial Revolution were not the factory workers. They were those in rural areas who were unable to migrate and take part in the new city life.

Old money fights back, using whatever weapons are available. Occasionally, they use guns and bayonets. More typically, old money restricts economic freedom and throttles the life out of the new middle classes by using trade laws, repressive taxes, and subsidies — whatever it takes to slow or stop their growing economic power. Few people realize the role technology is playing in an ongoing revolution until it's too late to stop it. The emperor's old toy doesn't look disruptive until it's in the hands of millions. Then come the laws banning, controlling, and restricting it. Horses only for the nobles. Books only for the priests. As we'll see, these attempts to control and restrict the technology of the Digital Revolution are central to our story.

In 1815, as the Industrial Revolution peaked, British landowners (the old money) enacted the Corn Laws to block the transfer of power to the new middle classes by taxing industrialization. The his-

torian David Cody writes[4], "After a lengthy campaign, opponents of the law finally got their way in 1846 — a significant triumph which was indicative of the new political power of the English middle class." By 1850, the Industrial Revolution was over and across Europe, power shifted away from landowners and towards the new urban middle classes.

In the early twenty-first century, the upper classes are business and political elites who accumulated their wealth and power over the last fifty years. The middle classes are all those who "got connected," soon to be most of world's population, and the lower classes are the shrinking few who cannot yet get on line. We will, over the next decades, see similar attempts by this generation of old money to throttle the growing power of this global digital middle class.

The Counter-Revolution Today

What is the twenty-first century equivalent of Britain's nineteenth century Corn Laws? How is old money fighting the revolution? There are two main strategies: property laws and simple repression.

The first is based on continuously extending the legal definition of "property" so that it appropriates any and all assets built by the digital economy. Property is entirely a political construction. Imagine an economy where upstream farmers have easy access to water and dominate agriculture. Adhering to the natural laws of cost gravity, technology for irrigation and flood control falls to free, and the downstream farmers, who previously lived in a swampy delta, start to prosper. Up to then, water is not considered property. Now the upstream farmers, who control the political system, enact a law stating that the water in a river belongs to whoever lives furthest upstream. The downstream farmers must pay exorbitant taxes or go to prison.

Political systems claim to do what is best for society. That is not how things happen. Laws are written by the powerful for their own benefit first, that of others incidentally. It's up to the downstream

4 https://en.wikipedia.org/wiki/Corn_Laws#cite_note-2

farmers to organize, gain power, and fix the laws. Democracy does not create balance in a society; it can only express its balances or imbalances.

In the early twenty-first century, an insipid set of copyright and patent laws are lazily and cynically bundled together as "intellectual property." These laws are designed — just like those water laws — to tax the new "digital farmers" and slow down or stop their growing economic and political power.

The second strategy is classic good-cop/bad-cop repression. On the one hand, we have the bread of cheap goods and the circus of "reality TV." On the other, we have the bloody hand of the wars on drugs, terrorism, piracy, indecency, and privacy. Our cities are blanketed with spy cameras, our networks monitored, and our police forces casually militarized. We label undesirables as dangerously anti-social: "drug criminal," "terrorist," "hacker," "pirate." Then we lock them up, torture them, use them as slave labor, and/or execute them. Those who raise a hand in defense of the undesirables or leak information about the state's excesses are tarred with the same brush.

Society is measured by how it treats those outside the mainstream. In 2011 in Norway, a man who killed 77 people for political reasons was labeled "insane" and treated as mentally ill. In other countries, he would have been labeled as a "terrorist" and tortured for years. Abuse of children is a terrible thing. Branding teenagers who send nude pictures of themselves as sex offenders, with life-long consequences, does not protect anyone. We are often so afraid of losing our bread and circuses and so quick to fear and hate others that we're ready to give up our neighbors without a struggle. We often clap as authorities drag away the wretched lawbreakers.

And the labeling continues: "extremist," "communist," "liberal," "union organizer," "intellectual," "atheist" — and the midnight knock on the door is for our parents, brothers, children, ourselves.

Torturers and brutes know no limits except those we place on them. That is, we cannot as society *expect* authority to behave itself

and then act surprised when it does not. The secret services will spy on us illegally. The police will detain and abuse vulnerable individuals illegally. This is how authority behaves when it is free of oversight. So in the long term, a peaceful society has to learn to regulate its police forces and spies, keep them in line, and moderate their behavior by force.

Creating the Future

Conflict defines us. It destroys us, or makes us stronger. It's out of conflict that new political structures emerge, for politics is essentially about organizing disparate groups and factions to win power through some kind of conflict, and then keeping these groups in balance to prevent further conflict. The new political structures of the twenty-first century will be unlike any we've ever seen before. Today, we have the seeds, and already they are international, anonymous, decentralized, self-organizing, fast, and accurate.

When we say that the Internet "removes borders," this will one day literally be true. Two generations from now, the political structure of nation-states will be as quaint as medieval city-states, shires, and dukedoms. Just as with the Corn Laws in nineteenth-century Britain, the injustices of the counter-revolution are driving a generation to political activism. Perhaps the first and most significant digital activist was Richard Stallman, who in 1989 nailed the GNU General Public License (GPL) to the church door. I'll come back to Stallman's story in "Magic Machines". Today, activists across the world are occupying the squares and streets of our cities, demanding an end to crony politics.

I started to decrypt and document the dynamics of the digital revolution and counter-revolution in 1999, and then in 2005 took over as president of the Foundation for a Free Information Infrastructure[5] (FFII), a European activist network that fought software patents. We built websites and campaigns, organized conferences, and wrote laws.

5 http://www.ffii.org

They called us "anti-business" so we wore suits and brought countless small business owners to speak. We tried to convince emerging Internet giants to support us.

We were five years too early. At the time, Google had a single solitary patent lawyer and could not take the patent problem seriously and help us. While we defeated a huge army of lobbyists in the European Parliament in 2005, it was a temporary success. Every committed FFII activist burned out and had to go back to a "normal" life.

The FFII is more or less shuttered now. It spawned successors like April[6] and imitators like End Software Patents[7]. Younger minds, unhampered by twentieth century conventions of style and reputation, continue to deconstruct the concept of "organization." They are creating new activist communities capable of challenging entire governments. From FFII to Anonymous, they are the Anti-Corn-Law League of the digital revolution.

The scene is vast and global. While in the nineteenth century, political change could be triggered by a single event in a single city, today's political structures reach into every pocket in the world. There is no dividing line between the battles over the occupation of Tahrir Square in Cairo and the endless patent lawsuits fought in the Court of Appeals of the Federal Circuit in Texas. "The odds are on the cheaper man," said Rudyard Kipling[8]. Cost gravity can't be stopped, except by burning the libraries and murdering every person with an education, and even that only pauses things for a generation. It has been tried in Soviet Russia, Uganda, Cambodia, Rwanda, and North Korea.

As the official site of the UK Parliament notes about the Anti-Corn-Law League in the late-1800's: "*Growing pressure for reform of parliament in the eighteenth and nineteenth centuries led to a series of Reform Acts which extended the electoral franchise to most men (over 21) in 1867.*" The repeal of the Corn Laws was just one

6 http://www.april.org

7 http://endsoftpatents.org

8 http://en.wikisource.org/wiki/Arithmetic_on_the_Frontier

part of a wholesale transfer of power from the old to the new. The same will happen in the post-industrial world.

Chapter 1. Magic Machines

Far away, in a different place, a civilization called Culture had taken seed, and was growing. It owned little except a magic spell called Knowledge.

In this chapter, I'll examine how the Internet is changing our society. It's happening quickly. The most significant changes have occurred during just the last 10 years or so. More and more of our knowledge about the world and other people is transmitted and stored digitally. What we know and who we know are moving out of our minds and into databases. These changes scare many people, whereas in fact they contain the potential to free us, empowering us to improve society in ways that were never before possible.

From Bricks to Bits

During the Industrial Age, many corporations were born and grew large, becoming what we see today as "old money." This established group tends to view the wilder aspects of the digital economy as a threat. In fact, it often directly tries to control, slow, or reverse technological progress. It's a safe bet that despite its best efforts, every product of the human mind that can be digitized, will be digitized. We've already crossed the digital horizon in many industries and the rest will follow. Whether it be the notes of a new symphony, the design of a new pair of jeans, or the frames of a subway surveillance camera, human culture is ultimately going to end up as one very long number: a stream of bits. This is a historic inevitability.

Knowledge has largely moved on line, with Google acting as the general index and Wikipedia and Facebook as the aggregates of human knowledge. Who you know is as important as what you know. Business has moved on line in many cases: email, VoIP, wikis, mobile

phones, video chats, and virtual teams working for virtual companies selling virtual products to virtual customers for virtual money.

Digital entertainment products — music, video, games, social networks, pornography — are the main attractions of digital society to many people. Art students in the rich world switched to easier "new media" like video in the late 1990's and early part of the twenty-first century. Analog culture — typewriters, board games, printed books, handwritten letters — are becoming antiques. Collect those postcards, because your kids won't ever receive one.

When culture becomes digital, it's more than just a technological shift. With this shift, we also see new behaviors emerge. Take the music industry as an example. It used to be a top-down, industrial economy in which large firms delivered products to the market and small firms wanted to become large. Today, the avant-garde music industry consists of DJ mix communities centered around a handful of artists. Scale and growth means reaching more people, not hiring staff and buying larger offices. Music has always been language. When that language is digitized, a group of underground DJs with computers are more creative and powerful than the largest music business. Not only are bricks and mortar irrelevant in the digital economy, they are a handicap.

Cost Gravity and the Digital Petri Dish

In 1965, Gordon Moore, the founder of Intel, wrote:

> *The complexity for minimum component costs has increased at a rate of roughly a factor of two per year... by 1975, the number of components per integrated circuit for minimum cost will be 65,000. I believe that such a large circuit can be built on a single wafer.*

Moore's prediction that chips would double in capacity each year became known as "Moore's Law." At the time, he predicted that the rate of exponential increase would last about 10 years. It has in fact lasted over 40 years — though Moore's 12 months became 18 — and

shows no signs of decelerating. Chips (and disks, which follow the same curve) are the soil in which our digital culture grows, and we've seen that space double every year-and-a-half for the last half-century. That's an increase of 4,000,000,000 times.

It was not always like this. Space for the digital culture was limited and painfully expensive for a long time. When I bought extra memory for my first computer — a Commodore VIC-20 — in 1981, the bulky expansion pack provided me with 3,500 bytes of memory and cost 50 pounds. As I wrote my computer science degree thesis (a fun little programming language), I had to strip all the comments out of my software source code so that I could fit it on a floppy disk. The benefit of this was that as a young programmer, I learned how to make software that was lean and mean. The cons of this are obvious.

In 2013, as I write this, $10 buys me a 32GB memory card. In 2015, as you read this, that ten-spot will buy a 64GB, and by 2022, as you read this again to see how wrong I was, it will buy a terabyte on a chip.

Let's put that into perspective. As a writer, I can produce 10 pages of finished text in a day, which is about 30K bytes. I could fill the Commodore's 3.5K memory pack in about 1 hour. It took me about 3 months to fill the 170K floppy on which I stored my thesis. It would take me about 32 lifetimes of non-stop writing to fill my cheap little memory card.

It is significant that we've passed a point where space for the digital culture has changed from a luxury to a paper-cheap commodity. The cost of capacity — disk, memory, network, processor — has long been a limit to purely experimental or not-for-profit projects. By 2004 or so, there was a glut in capacity. A new wave (aka Web 2.0) of experimentation and social growth started, based on the availability of close-to-free resources for any individual or team with an idea.

I've observed that Moore's Law applies to much more than silicon: it applies to all technology, and always has applied. I call this general law "cost gravity": the production cost of technology drops by half every 24 months, more or less. Ignoring materials, labor, distribution,

marketing, and sales, the cost of any given technology will eventually approach zero.

For instance, the other day I bought a surprisingly cheap little black and white laser printer. The quality is impeccable; it's silent and fast. I recall the first consumer laser printers, which were expensive, huge, noisy, and slow. While it's nice to see things improving over time, it struck me that we could compute the cost gravity of laser printers quite easily. You can repeat this measurement with any technology that you can compare across two or three decades.

We will compare the HP LaserJet Plus, introduced in 1985, printing 8 pages per minute at 300x300 dots per inch, with the Samsung ML 1665, from 2010, printing 17 PPM at 600x1,200 DPI. When they were introduced, the HP cost $4,000 and the Samsung $50. Past 2010, black-and-white laser printers became so cheap that price "noise" makes accurate measurement impossible.

First, we adjust for inflation. That $4,000 in 1985 is just double in 2010 dollars, at $8,000. Next, let's adjust for technical specifications. The Samsung prints twice as rapidly at eight times the resolution and is about a quarter of the size. So I'm going to rate it at 32 times better, technically.

If there were no cost gravity at work (gravity of 0%) — and assuming that we're paying proportionally for technical quality — that original $4,000 printer would cost around $250,000, which is 32 times the price, doubled for inflation. If cost gravity were 10% per year, today's little printer would still cost $18,000. A cost gravity of 29% per year brings us to the 2010 price. That's a fall of about 50% every 24 months (0.71 x 0.71). $50 probably represents the bottom of the price curve: effectively zero. Technical specifications will improve (WiFi, color, longer-lasting cartridges), and then Korean and Japanese manufacturers will stop making them.

You may be wondering, then, why all old technology isn't literally free? Well, immaterial products do become free. Material products, however, are not just raw technology. They also require raw materials,

time, energy, and knowledge. A fine wine is expensive because it depends on rare raw materials, as well as knowledge, time, and scarce land. Green beans grown and handpicked on the hills of Kenya are expensive to western consumers because they must travel a long distance rapidly, which costs energy.

Cost gravity is what keeps the digital world alive: as our digital universe doubles in size every two years, the hardware it depends on falls in price by half every two years. For example, the hardware budget for Wikipedia has remained constant for years even as the size of the project has grown exponentially.

What drives cost gravity? The software industry, which creates purely immaterial products, shows how this process works. Software represents distilled knowledge about how to approach specific types of problems that can be solved using general-purpose computers. Collecting this knowledge is expensive at the start because it means fishing it out of individuals' brains. People need to travel, meet, talk, and think together. Once that's done, it is almost free to distribute, share, and remix the resulting knowledge.

So the digital economy has these rapid cycles where new products move from costly luxury to free commodity within one or two decades. Email was invented around 1980 and was available to very few privileged people. In 1990, my professional email account cost me about EUR 1,200 a year — more than my rent! By 2000, email was widely and freely available to everyone through web services like Hotmail.

The digital economy is built around either accepting or distorting this process of cost gravity. There are many ways to make a lot of money in the digital economy. One way is to create a company based on a not-yet-commoditized product and sell it to a larger, less agile firm (Hotmail, Flickr, YouTube and many others followed this model). Another is to make and give away products that other (slower) firms are still trying to sell, and use this to open the market to new services (Google does this very well).

A third approach is to create your own captive society and force it to use your products where, without real competition, prices can remain artificially high (Microsoft and more recently Apple are good examples of this). Finally, you could sell luxuries and fashion to people who have lots of disposable income (Apple is a fine example).

Cheaper digital technology also affects the larger economy. Transport gets more efficient, and cheaper. Production becomes automated and cheaper. Administration becomes more efficient, automated, and cheaper. The rapid global spread of digital technology is a principal cause of the growth in global prosperity over the last decade.

The First Law

The Internet — the fabric of digital society — was born on 7 April 1969, a few years after Gordon Moore coined his law. The event was the quiet and rarely celebrated publication of a "request for comments" on something called the "HOST software." The document, simply called "RFC001"[9], says:

> *During the summer of 1968, representatives from the initial four sites met several times to discuss the HOST software and initial experiments on the network. There emerged from these meetings a working group of three, Steve Carr from Utah, Jeff Rulifson from SRI, and Steve Crocker of UCLA, who met during the fall and winter. The most recent meeting was in the last week of March in Utah. Also present was Bill Duvall of SRI who has recently started working with Jeff Rulifson.*

Crocker, Carr, and Rulifson are not household names. Steve Crocker and his team invented the Requests for Comments, or RFC series. These documents became the laws of the Internet, specifying every standard in a clear form that was freely usable by all. These were spectacularly successful standards by any measure. They were implemented in hundreds of thousands of products and have survived for forty

9 http://www.faqs.org/rfcs/rfc1.html

years with no sign of decay. The RFC system did not only define standards for protocols, it also defined rules for the legislative process itself.

Today, despite this success, it is becoming harder and harder to make new protocols and standards. There are too many billions that depend on controlling, taxing, and corrupting standards. Patents are a major threat. The calculation is simple: imagine if email had been patented — how much money would the patent holder (let's call him the "inventor" or "job creator" for effect) have earned? If email had been patented — which happily it was not — then we would have suffered two decades of stagnation and suspension of cost gravity.

This has happened often in history, notably during the Industrial Revolution, with James Watt's steam engine patents. As Michele Boldrin and David K. Levine wrote, in their book "Against Intellectual Monopoly"[10], "During the period of Watt's patents the United Kingdom added about 750 horsepower of steam engines per year. In the thirty years following Watt's patents, additional horsepower was added at a rate of more than 4,000 per year."

Any expensive product or service that is widely used, yet immune to cost gravity — such as medicines or mobile phone calls — is protected by a patent cartel. If silicon is the space in which digital society grows, knowledge is its blood, and software its muscles. Patents make it illegal to reuse knowledge and (despite the old rhetoric of the patent industry) kill the broad incentive to invest. We'll come back to patents later. For now, I'll leave you with that glimpse of how dangerous they are.

A Brief History of the Internet

I will summarize the history of the Internet thus: a generation that grew up with computers in college and university went out into the real world and colonized it with their freaky and ultimately accurate vision of what was possible with ever more cheaper and faster com-

10 http://levine.sscnet.ucla.edu/general/intellectual/against.htm

munications. It took only four decades to go from three terminals on a local network to almost seven billion mobile phones[11], of which two billion are smartphones, on a global network.

In the 1960's, mainframes ruled. These were huge expensive machines run like private empires. People were experimenting with simple networks. In 1962, I was born, and someone also invented network packets. These are like envelopes of information that could be sent around different routes to get to their destination. The military began developing packet-switched networks that could survive a lot of damage. Around 1965, people invented mainframe electronic mail; in 1969, the first RFC was written; and in 1971, the @ sign was born.

The first Internet was actually built out of smaller networks like Arpanet, which had a whopping 213 hosts in 1981, and Usenet, which had 940 hosts by 1984. The Internet doubled in size every eighteen months. The Internet Protocol (IP) made it possible to route packets between networks (not just inside single networks) and after Big Brother failed to appear in 1984 (except in Apple adverts), the Internet grew into a worldwide research network that reached most places except Africa.

The Internet's dark side as we know and love it — spam, viruses, porn sites, download sites, credit card fraud, identity theft, malware — blessed us with a brief preview in 1988, when the first worm flattened the academic Internet. We had to wait until 1990, when commercial restrictions on Internet use were lifted; and then 1991, when Tim-Berners Lee invented the web at CERN, in Geneva; and finally 1993, when Al Gore found funding for the development of a graphical web browser named Mosaic. Suddenly, any fool with a PC and a modem could get on line, and The Real Internet was born.

It still took Microsoft more than two years to catch on. Rather than recognize the new Internet, it stubbornly rolled out its own "Microsoft Network" that hardly talked to the Internet at all. Win-

11 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

dows 95, despite being the most installed software of 1995 after the game Doom[12], had no Internet functionality whatsoever. When Netscape became the dominant browser, Microsoft realized its mistake, and brought out a patch for Windows 95 and a branded version of Mosaic. It then slowly beat Netscape to death by giving its browser away for free, destroying Netscape's market, and establishing itself as the new bully on the Internet block.

In 1998, the domain name system was privatized and opened to competition. Suddenly, the cost of buying a dot-com name fell to rock bottom. Not surprisingly, lots of people bought dot-com names. Sensing a gold mine, the island kingdom of Tonga started selling .to names, and soon every country was selling its "national" domains to all and sundry. The coolest were probably .tv and .fm, though.

Also in 1998, Google was founded, and soon their revolutionary concept of "it works the way you expect" made them King of the Search Engines. Once upon a time, the list of all websites was twenty pages long. I still have a book that has the entire World Wide Web printed as an appendix. Then the list got too long to print and sites like Yahoo! organized them into categories.

Then the category list got too large to keep updated, and Lycos invented the full-text search. This was too slow, so Digital Equipment Corporation built a natty search engine called Altavista to show how to do it properly. The results for any search got too long, so Google invented the ranked search, which pretty much fixed the search issue. Google also threw all the clutter off the main page. Less is more.

The dot-com boom bubbled in 1999, driven by the dream of cheap access to millions — no, billions — of consumers. Investors threw huge amounts of money at firms whose business plan typically went: "*1. Give people something free. 2. ??? 3. Profit!*" In 2000, the dot-com bubble burst, mainly because big firms had spent so much cash on solving the millennium Y2K "crisis" that they had to freeze all new IT spending for two or three years. Big IT firms' profits fell, investors

12 https://en.wikipedia.org/wiki/Doom_(video_game)#Release

panicked, the stock market collapsed, and so did most dot-com firms. Most of those companies' business plans were empty anyway.

In 1999, Napster started to let people trade songs on line. It was blatantly illegal and incredibly popular. Napster was almost immediately sued and shut down by lawsuits in 2001, the same year that Wikipedia, the blatantly legal and incredibly popular shared-knowledge collection website, was launched. After shrugging off many years of contempt and ridicule for allowing anyone to edit pages, Wikipedia made Encyclopedia Britannica redundant by around 2005.

Around the Millennium, it was not yet clear that the digital revolution was real. By the late 1990's, the widespread use of computers at work had lowered — not raised — productivity. Everyone was playing Solitaire instead of worrying about the coming end of the world. The dot-com crash seemed to prove that brick-and-mortar was still the real world and that "digital mindshare" was a hoax.

From 1999 to 2004, huge swathes of the post-industrial service economy quietly continued to go digital. The fast fiber optic cable links from the US to India that were used in 1998-99 to do Y2K conversions became the portals for massive outsourcing. And as businesses quietly off-shored and reorganized around an ever cheaper global communications network that let them move help desks to Bangalore and insurance claims processing to Haiti, the second Internet boom, aka Web 2.0, exploded sometime around 2003-2004.

Ironically, given their reluctance to innovate and their dependence on captive markets, it was Microsoft that triggered Web 2.0. In 1999 they released a small toolkit called XMLHTTP that let web authors escape the click-driven box of the classic web page. Suddenly pages could update themselves, and started to look like real applications. Google flew with the idea, using it for Gmail and Maps, and "Ajax" was born. Flickr and YouTube, launched in 2004 and 2005, mixed the pretty new Ajax technologies with community and self-created content to create massive hits.

The Internet has continued its explosive takeover of technical, social, economic, and political life. Pretty much every person on the planet is connected — if not directly, then by immediate proxy. We amplify our lives through Facebook, Twitter, massive multiplayer games, email, chat, Skype. The only people who are not on line fairly regularly with a diverse network of contacts are too poor, too old, too young, or (and I'm speculating here) young men who are so socially isolated as to present a "lone wolf" threat.

Digital political activism has never been more aggressive, confident, and successful as it confronts abusive cults, authoritarian governments, and dictators, and spreads its philosophical anarchist vision of the future[13]. Anonymous, the faceless un-organization that grew from image-sharing forums like 4chan.org, is arguably[14] one of the most powerful organizations on earth.

What Drives Digital Society?

Technology is not inevitable. Powerful drivers must exist in order for people to keep pushing the envelope and continue demanding more and more from a particular field of knowledge. In my view, digital society is driven by several factors.

Cheaper Communications

The first and most important driver is our demand for ever cheaper and easier communications. In 1960, we could perhaps keep in touch with 50 people by meeting them face-to-face, writing them letters, and sometimes giving them a phone call. Very well organized people kept indexes of people they knew. Today, we can keep in touch with tens of thousands of people, and computers have become social memory banks. They help us track who we know, in what context, and what we've talked about.

---

13 https://en.wikipedia.org/wiki/Philosophical_anarchism

14 http://news.nationalpost.com/2012/05/12/insider-tells-why-anonymous-might-well-be-the-most-powerful-organization-on-earth/

All of human society depends on communications. When we can reach a hundred times more people, all of society is turbocharged. The demand for communications is intense and apparently limitless. In Tanzania in 2007, there were 150,000 fixed phone lines, representing the pre-digital phone network, and already 2 million mobile phone subscribers. In 2011, more than twenty million[15] Tanzanians used mobile phones.

Entertainment

Humans are neotonous animals: we act like kids for most of our lives. It was our own invention of fire that gave us cooked food and freed us from needing the large adult ape jawbone. A smaller jaw and cooked food meant a thinner and lighter skull, which allowed more space for the brain. Since humans learned to make fire, every labor-saving invention has gradually reduced our need to be self-sufficient wild animals and turned us into a self-domesticated species.

Like our dogs, which are domesticated and neotonous wolves, we play even as adults. The Internet has always been a fertile space for imaginative ways to have fun. Chatting with friends, on-line games, porn, aimless surfing, shopping, swapping music and films; the Internet has a powerful pull on our baby ape nature.

Communities and Social Networks

Since the earliest bulletin board systems, humans have been drawn to join and hang out in on-line communities. Since its birth, the Internet has offered a rich world of special interest groups. Whatever your passion, the Internet provides hundreds, even millions, of people who share it, right at your fingertips. Pre-Internet commercial networks like Compuserve and AOL essentially sold "community" as their main product, and today this drives big sites like Facebook, Twitter, Reddit, and YouTube.

---

15 http://www.africanbusinessreview.co.za/news_archive/tags/canada-s-international-development-research-centre-idrc/fifty-percent-tanzania-s-population-usi

Business

Even though the Internet opened to commercial use only in the early 1990's, it's become an essential tool for all industries. Obviously, communications is a big driver for business. Email is very cheap. We also adopted the Internet because it became an excellent research tool, a cheap way to handle clients' problems (via forums and wikis), a cheap way to do marketing and sales (websites), a cheap distribution channel for digital goods (especially for the software industry), and a cheap backbone for virtual organizations.

In 1996, one of our large clients was shocked when we proposed to make a new application using the web. Their disbelieving response was, roughly, "this could never work." By 1999, everyone was trying to move their business on line, and despite a rough start, most US and European businesses were firmly on line by 2003 or so.

Politics

The citizens of digital society have over time organized themselves to fight off the threats they saw from hostile organizations, and these organizations became political structures that used the Internet in an extreme fashion. When I took over as president in 2005, the FFII had more than 500 mailing lists and 20,000 wiki pages. In the US presidential elections of 2000 and 2004, the Internet played a big role in reaching people, exchanging news, and organizing people. The US presidential elections of 2008 and 2012 were organized and waged in the blogs and forums more than on TV. The Boston Marathon bombings of 2013 were reported — and misreported — in real-time on Twitter and Reddit, and more people followed and created the stories there than on TV.

Globalization

Despite the emotions that the "G" word still invokes, we've awoken in a global society where it's almost as easy to reach someone in Bangalore as it is in Brussels. Keeping in touch with friends abroad used to be arduous and costly; now it's easy and free using email, Skype,

Facebook, and Twitter. The same goes for business: cheaper communications enable US businesses to outsource massively to the other side of the planet. If the dream of real free trade without the price fixing and geopolitics that still typify today's markets ever comes true, it'll be largely thanks to the Internet.

Defiance

Rarely discussed, yet present in the minds of many early Internet users, was a feeling that they were changing the world. One small step at a time, we've deconstructed industrial-era industries like telecommunications, insurance, and travel. Banking, retail, and academia are slowly and surely following. Another decade or two, and school holidays will disappear. Politics is seduced by the idea of building new movements. The feeling of power and freedom that comes from helping to bury the past is addictive to many people. Perhaps it's a combination of rebellion and faith in a bright, shiny future.

Of Mice and Dinosaurs

The thing we call "a business" has been revolutionized in the four decades since that first RFC broke the ice. A serious firm used to require physical premises, stock, notaries, salesmen, equipment, directors, vice presidents, secretaries, a mail room, printing service, human resources, middle managers, regional offices, regional managers, and so on. The cost of starting even the smallest firm was so high that people were compelled to make complex financial arrangements to collect the necessary capital. The high price to society of failed businesses meant that every aspect of starting and running a business was heavily regulated, which added to the cost and complexity. Most people had no choice except to work as employees for existing firms.

Today, of course there are still firms that look exactly like their predecessors of the last century. These are the dinosaurs, and their size and weight disguise their weaknesses. For every large firm that occupies an impressive building in the "business district," there are tens of thousands of entities that operate from cyberspace with no offices,

formal construction, or capital. Most scarily for classic businesses, there is a single, increasingly level playing field. Clients barely care about the impressive offices. The high costs that used to act as a useful barrier to entry are now just overhead.

Let's look at the practical realities of starting a small business today:

- We don't need impressive offices because customers don't care much about seeing how solid and well established we are. It's all about the ability to deliver and building a long-term (Internet-based) reputation. The perception that a real firm must be backed by a real building died in theory around the turn of the millennium, and in practice perhaps five years later. All we need now is a postal address, fast Internet access, coffee, and temporary meeting spaces.
- We don't need to hire employees or have a human resources department because more and more skilled staff choose to work as independent contractors or small businesses. Contracting and partnerships are more flexible than classic employment — especially in Europe, which still struggles with an over-regulated labor market. Europe's heavy laws on permanent staff were effective tools against labor abuse in the last century. Today they're increasingly punishing for small, agile businesses.
- More of our communications infrastructure (websites, email, archival) can be handled by free or low-cost managed services. This means we don't need dedicated computer systems or support staff.
- Resources and information are available on line. This means we don't need staff to do research. For example, we used to need to pay a travel agent to organize travel. Today, we can do it ourselves, so trivially that we forget what a chore this used to be.
- The cost of creating legal entities is falling, driven by a very competitive US market. Europe still lags behind. Some smaller European countries such as Estonia and Macedonia are positioning themselves as the Delawares of Europe (not to be confused

with tax havens like Cyprus, which have as their model secrecy and low taxes rather than simple efficiency).

- Government departments are increasingly using email instead of paper, and accepting tax returns and other reporting via the Internet through standardized formats. This reduces the need for accountants and other middlemen.
- Products have gone digital in many domains, eliminating manufacturing costs, and sharply reducing the costs of packaging and marketing. When physical products need to be built, there are many "assembly" firms that will make these; dedicated manufacturing is a thing of the past.
- Funding, which used to be sought from a few significant investors, can now be sought directly from prospective buyers through crowdfunding platforms like Indiegogo and Kickstarter.
- And of course, as I've explained before, the costs of communications, both internal and external — the biggest cost of the classic firm — have been reduced to near zero.

Let me take a concrete example of a young business that wants to develop and sell a new high-tech product. The core design and engineering team consists of perhaps 10 people. This hasn't changed. In the classic firm, this team would need about 100 further people to help develop, package, market, sell, and support a product. More products would mean more people. A successful product would mean growth — not of core engineers, rather of salesmen, middle managers, and support people. Today that team needs no further support at all, and can handle large successes without requiring expansion.

And so we see something totally unique in the history of commerce: the largest firms on the planet face direct competition from tiny start-ups that can move rapidly, experiment with high-risk strategies, adapt overnight, and grow large to fill new areas before large firms even realize those markets exist. Many competitors of established businesses do not even consider themselves "businesses," rather "projects" or "communities." This makes them hard to fight us-

ing the traditional weapons of the marketplace, namely marketing, aggressive pricing, buyouts, and so on.

Let's look at some major old industries that cling on, and see what challenges they're facing from new forms of organization:

- The old news industry faces social networks, WikiLeaks, Reddit, mobile phones.
- The old advertising industry faces Google.
- The old music industry faces file-sharing, home studios, and mixing.
- The old telecoms industry faces Google and Facebook, Skype, email.
- The old academic industry faces Wikipedia.
- The old software industry faces free software and ad-sponsored mobile applications.
- The old television industry faces YouTube and BitTorrent.

From looking at this breakdown, I conclude that many industries have passed a "digital boiling point" where their industrial-age products and services are turning into digital vapor, and like frogs in the pot, they are often slow to make the leap to safety. Will the music industry ever embrace file sharing? Will academia ever learn to embrace Wikipedia? Perhaps the key to answering these questions is to understand that the real competition does not simply come from smaller, faster, lower-cost organizations. These merely drive down prices. The real competition comes from radical new approaches to the very nature of work, which have the potential to destroy existing markets as they create new ones.

The Establishment Under Assault

In the early 1990's, I wrote an article imagining the future. "I want to be able to record the bytes off my music CDs, which are digital, and compress them," I wrote. "Imagine, my own digital music jukebox." This was a year or two before CD rippers and MP3 compression became available. Already music studios had gone digital and no one ser-

iously doubted that CDs would beat vinyl. Today I can hold the digital contents of my old thousand-CD collection on a tiny memory card. Music has become the epitome of the digital good, exchanged and collected by billions of people, while the music industry goes through a slow, complex, and painful rebirth around this new reality.

It's instructive to look briefly at the digitization of the music industry, because the same process is happening in many other industries. DVDs replaced the VCR, and video followed music onto the Internet as a shareable artifact of popular digital culture.

The music industry moved to digital technology for its own production processes in the eighties. Sony and Philips published the CD-ROM audio standard in June 1980, consumer music went digital, and consumers found themselves with a cornucopia of new digital content, albeit at a higher price. Music CDs were typically priced 25% higher than LPs and sold as higher-quality luxury items. The price of producing CDs fell, of course. However even when CDs cost under a dollar to produce and distribute, they still remained very expensive in the shops.

The perceived unfairness of this pricing model gave many people the feeling that Internet music "file swapping" was justified. Later, the on-line exchange of movies, TV programs, and music simply became so convenient and widespread that it normalized. Audio CDs were not initially "digital goods" because we could only play them in CD players that roughly imitated LP players. However, in the mid-1990's, home computers became powerful enough to "rip" and store these digital goods, squeezing them into more efficient forms (the MP3 format). And by the late 1990's, the Internet was capable of transporting these files, resulting in the birth of mass-market file sharing networks.

The first such network, Fanning and Parker's Napster, lasted three years from launch to bankruptcy and liquidation, hitting 26.4 million users and multiple music industry lawsuits in the process. Its successors (FastTrack, Gnutella, Kazaa, WinMX, AudioGalaxy) were also

smashed by music industry lawsuits. In a pattern we see many times, stamping down one pirate business created dozens of new ones to take it place. Killing Napster turned a handful of networks into dozens, then hundreds, mostly using the BitTorrent peer-to-peer (P2P) technology.

It has proven impossible for the music industry to kill file sharing, yet they have tried endlessly, declaring "war on downloaders," suing file sharers, buying laws to criminalize copyright infringement, and on and on. A Russian site, AllofMP3.com, launched in 2000, was very successful at selling music cheaply by the megabyte. It did not pay royalties to the US music industry. After many years of conflict with the established music industry, including suspension of its credit card payments — heralding a form of attack that would be used much later against WikiLeaks — it was finally killed in 2008 by direct political pressure from the White House all the way to the Kremlin.

During the long fight between the industry and the pirates, Apple managed to produce the first industry-sanctioned model that let users easily buy digital music and play it on their portable players. It was hugely successful both in making it an easy experience for users and a profitable one for itself and its music industry partners. In 2004, Apple's stock was around $10; it peaked at over $600 in 2012, and digital music played a major part in their success.

So after a lost decade of lobbying and lawsuits against every plausible new model of music distribution, the music industry finally accepted that the mass market wanted to play music via the Internet and opened up to new business models like Spotify's all-you-can-eat service[16].

In the end, all we wanted was a free choice of music, always available, with a "Play" button on our phones, tablets, and laptops. It was never about getting something for free as such, rather about convenience and choice, and it turns out we're mostly happy to pay for this. Indeed, downloading and sharing free music was never a cheap

16 http://www.spotify.com/

hobby; it needed large hard disks, fast connections, and powerful PCs. That people were willing to spend quite a lot to do this disproved the "piracy is theft" claims.

It's very much the same story with television and cinema. For a decade, these industries have watched the growth of faster networks and larger hard disks with dread. "The Internet is going to eat us alive," quoth the movie industry. It happened to music, so clearly video was next.

Except that it didn't happen. The incredible volume of television shows and movies shared via BitTorrent networks didn't kill the global appetite for moving pictures; it spurred it on. As for music, we downloaded because there was no other way to get the convenience and choice, and shared out of disgust with the state of affairs. And as for music, the movie industry (more than the television studios) used the courts and legislators instead of simply giving the market what it wanted.

Today, the TV and movie streaming service Netflix eats a full third of peak Internet traffic to homes. The most pirated television shows are also the most watched on the for-profit networks. What every software project has known for decades is now apparent to the movie and TV studios as well: the real threat to long-term survival is not piracy. It is obscurity. Piracy didn't kill the moving picture. It probably saved it from disappearing among the many other digital attractions.

It's All in the Remix

The software industry is arguably the one with the best record of reinventing itself multiple times over during the last decades. Innovation in this industry tends to bubble up from small, extremely competitive teams and businesses, with slow adoption by larger businesses over time. For example, around 1985-90, the dominant business model for tiny software firms was "shareware," software you could try for free and buy if you wanted it. Today this is how the largest firms like Oracle still sell their software.

The leading edge of software development often sets the tone for other knowledge industries. A clear example of this is how we solved the "software crisis" of the late twentieth century.

In 1987, Fred Brooks, a leading expert of the problems of the software industry, famously wrote[17] that "*we see no silver bullet. There is no single development, in either technology or in management technique, that by itself promises even one order-of-magnitude improvement in productivity, in reliability, in simplicity.*"

Brooks listed a number of steps that might solve the software crisis. In 1987, the software industry was already seen as vital to the economy and was considered to be in crisis. We could not, at the time, produce sufficient software of high quality and low price to satisfy demand. Brooks was previously head of a major IBM project to write a new mainframe operating system. The experience was one of trying to manage ever-expanding budgets and failing deadlines. It left him deeply skeptical of the software industry's capacity for self-improvement.

He wrote, in his landmark 1975 book, "The Mythical Man Month" that "*adding manpower to a late software project makes it later*," a lesson that Microsoft would have been wise to understand when they built Windows Vista over five long years from 2001 to 2006. Fred Brooks was technically right when he said "no single element" could solve the software crisis. Yet like everyone at the time, he missed the point and failed to see the oncoming revolution in software development. History shows that two elements combined to create a thoroughly effective silver bullet.

The first was the relentless pressure of cost gravity, which from 1975 to 1995 brought the cost of software development infrastructure — computers and networks — down by 1,000 times, and by 2015, a million times. Cost gravity is what makes the Internet possible at all. Without it, the boxes that route today's traffic around the world would be the size of airports and consume more electricity than entire

17 https://en.wikipedia.org/wiki/No_Silver_Bullet

cities. Actually it's a nonsense vision: without cost gravity, we'd not even be here.

By 1995, it had become easily possible for individual programmers to buy computers and link them together using email, the file transfer protocol (FTP), and other young protocols like the hypertext transfer protocol (HTTP). So while Fred Brooks's IBM had to bring expert developers together in huge research facilities, the Internet allowed the same developers to work from anywhere, to create flexible ad hoc teams, and solve problems in much more intelligent ways.

The second element is what I consider one of the key technological developments of the twentieth century digital revolution, which was a new private contract for collaborative development called the GNU General Public License, or GPL[18]. It was this document, this license, that finally solved the software crisis.

I doubt that Richard Stallman, the man behind it, had such lofty goals. As far as I can tell from his writings at the time, he simply wanted to prevent volunteer efforts — quite common in the software sector since its first days — from being converted into closed commercial products, locking out the original contributors. Stallman also inadvertently fixed the software crisis, spelled the end of the classic software industry, and laid the foundations for the twenty-first century software industry.

The GPL is a model for a broader kind of collaborative innovation that people call "remixing," which we see in other sectors such as music and digital art. Remixing is a surprisingly effective way of producing certain kinds of knowledge goods. It occurs when a group of creative people agrees to allow each other to reuse ("remix") their work into new forms, freely, and under the condition that any new mixes are available to everyone under the same conditions. It is a "share-alike" form of collaboration that feels comfortable to many groups and is widespread in society, once we look beyond the gates of media businesses.

18 https://en.wikipedia.org/wiki/GPL

Creative groups often adopt remixing conventions without formality and legalisms. For example, many music scenes consist of DJs who remix original material with new samples, lyrics, and their own sounds. Or, a group of graphic designers might swap material and combine each other's work. Lawyers tend to remix contracts without guilt. A knitting circle will share patterns and techniques. Gardener's clubs exchange tips, seeds, and plants. Doctors exchange remedies and diagnostics. Farmers share solutions to animal husbandry and pest control. The fashion industry utterly depends on remixing.

Remixing is a natural way of working that has a long history with roots in our social psychology. Sharing one's ideas and work is good for everyone. No one likes a hoarder: imagine the reaction to a doctor who discovers the cure for a disease — using all the knowledge given to him by others — and refuses to share his new knowledge with others. He or she would be condemned as criminal.

The lust for money, especially in the form of business, breaks down this collaborative model. This can be an example of how the free market, which I generally like and respect, can work completely opposite to the interests of society at large. When businessmen get involved with commercializing a successful work, they have little choice — in the conventional business model — except to stop people from remixing the now precious work into new forms. It is of little consequence that the commercial hits are based on others' work. Informal sharing agreements cannot survive when the economic incentive to cheat is higher than the incentive to share.

Some types of work are deemed so "utilitarian" that they don't have copyright protection. This is the basis for the fashion industry, for example, where designs are copied without shame. Courts repeatedly refuse to punish those who copy designs for shoes and clothes, as long as they don't copy the trademark. The fashion industry is also an order of magnitude larger than industries that use copyrights. Software, despite being highly utilitarian, falls under copyright law and that makes it easy for businesses to close off soft-

ware source code. They can easily take software that is developed collaboratively, such as by students at a university, and create closed products that even authors whose work was used in those products cannot remix.

Stallman found the answer to this problem. He defined a simple license that put the remixing agreement into written form backed by copyright law, and made it much harder to cheat. The license says it is, "*designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.*" Licenses like this are easy to enforce, and the GPL has been upheld by courts in many instances.

The GPL is the dominant share-alike license for software. For music, photography, and writing, the Creative Commons project offers a whole raft of share-alike licenses (as well as other types) that "give everyone from individual creators to large companies and institutions a simple, standardized way to grant copyright permissions to their creative work."

When done properly, a remixing license is incendiary. First, it effectively prevents cheating, giving creators a strong guarantee that their work won't at some future date be taken out of the remix and perhaps even used to compete against them. Second, it allows the remix to scale (that is, grow to any size) by explicitly defining the rules so that complete strangers can collaborate. Confidence and scalability allow a group of friends who agree between themselves to grow to a community of thousands or millions who can work together in confidence.

In software, the GPL spawned a massive new remix, called "free software," commonly yet wrongly lumped together as "Linux." Free software is so abundant and of such high quality that the software crisis can be considered definitively solved. Noting that that 90% of

everything is crud, Theodore Sturgeon pointed out[19] that this did not detract from the quality of the other 10%. It is only firms that refuse to use this technique — like Microsoft, SAP, and Oracle — that still suffer the traditional high costs and delays of old-fashioned software development.

For a large-scale remix to be successful it must be one hundred percent *self-hosting*; that is, it cannot depend on any proprietary — legally unremixable — material at all. When a DJ makes the error of remixing in a little commercial pop music, their work cannot be legally distributed at all.

The remix definitely threatens established interests. More broadly, conflict between old and new is a constant, defining part of the history of digital society. Sometimes this conflict affects hundreds of millions of people. Nowhere is this more dramatic than in Africa, a continent that the Internet almost totally bypassed.

The Lost Continent Gets On Line

Poverty on Purpose

Let's start by asking a painful question often asked, and yet in my experience rarely usefully answered: *Why is sub-Saharan Africa so persistently and so stubbornly poor?* The conventional story is of Africa the Victim, a proud continent swindled by slavers and colonialists. And, simultaneously, at blame for its own situation, overpopulated and warlike, corrupt and tribal. These stories seem racist, bogus, and worst of all, useless.

I was born and raised in Africa, and have lived in, worked in, or visited both Congos, Kenya, Tanzania, Rwanda, Angola, Togo, Ghana, Nigeria, Burundi, and Uganda. My wife is Congolese, my father was a diplomat mostly working in Africa, and my sister is a professor of political science specializing in Africa. Yet in my whole life, I've never heard a satisfactory answer for this question. And its an important

19 https://en.wikipedia.org/wiki/Sturgeons_Law

question because Africa's poverty is the world's poverty. Africa's poverty shames us and also cripples us. Poverty can be profitable for a few. It cannot be profitable for the entire species.

The economist Jeffrey Sachs has argued[20] that Africa's geography — it is a huge landmass with few waterways and many barriers to transport — is one of the underlying reasons that this continent missed the Industrial Revolution. Sub-Saharan Africa (which I'll just call "Africa") is geographically challenged beyond most people's comprehension.

The World Port Source[21] shows the harbors and ports of every country in the world. No matter which figures you look at, you will discover bizarre comparisons. In 2013, the United Kingdom has 389 ports, while the US has 532. Japan has 292; China, 172. And then, let's look at the largest African countries and economies: Nigeria has 12, South Africa has 10, Ghana has 4, Kenya has 3, and Congo-Kinshasa also has 3.

The sheer lack of ports is easy to understand when you look at the map: the coastlines of Europe and North America, carved by rivers and glaciers, are very crinkly with hundreds of natural harbors. The coastline of Africa, old and continental, is mostly smooth. In "Faceless Societies", I will develop the hypothesis that as geography drove Europe towards prosperity, it drove Africa towards poverty.

It's not just bad geographic luck, however. When I checked these figures in 2008, here was the tally: UK had 279 ports, the US had 371, Japan 144, and China had 157. Meanwhile Nigeria had 12, South Africa had 10, Ghana had 4, Kenya had 3, and Congo-Kinshasa had 3. Nothing had changed for Africa, while the more developed countries nearly doubled their port numbers in some cases.

Let's look more closely at the figures. Nigeria, a country of 165 million people, has 12 ports. This breaks down into four "medium-sized"

---

20 http://www.earthinstitute.columbia.edu/endofpoverty/

21 http://www.worldportsource.com/countries.php

harbors, at Lagos and Port Harcourt, and eight small or very small ports. Belgium, where I live, has four "medium-sized" harbors, and also two "large" ones and a "very large" one at Antwerp.

A current expansion of the main Lagos Appa port, will bring it to 1.2 million twenty-foot equivalent units (TEU) per year[22]. A TEU is half a container. So, 600,000 containers a year, or 2,000 per day. It sounds like a lot. Antwerp, by comparison, has a capacity of 15m TEU per year, more than 10 times the amount.

The lack of import/export capacity in Africa is very profitable for those in power. There is little or no competition. If you want to use those ports, you have to pay the price. Most countries are literally captive markets. If I want to ship a container out of Brussels, I have the choice of dozens of ports fighting for my business; if I want to ship a container out of any city in Africa, I have the choice of paying through the teeth to the local rulers or trying to ship my container thousands of miles across poor roads to another crime outfit.

If we look more widely, we see that most of Africa's infrastructure — electricity, water, highways, schools, and communications — are mainly built by a local political and foreign corporate elite with borrowed money to serve their own interests.

Sachs says that geography is a major cause of poverty in Africa, and he's right. That's only the start of the story. Geography enabled the foreign corporate and local urban political elites to maintain a choke hold over the essentials of life. There was no other way to connect to the world except through a tiny handful of ports and the cities that grew around them. Control those precious gateways to the outside world, and a life of luxury is guaranteed.

Entire clans have made it their business, for generations, to control these gateways together with their foreign partners, and keep the choke tightly applied. Wars have been fought over and over for control of the port cities, because that was always where the money was.

22 http://www.thisdaylive.com/articles/expansion-boost-for-nigerian-ports/140227/

Enabled by geography, Africa's enduring poverty resulted from this easy choke hold, which has survived for a hundred and fifty years. In some places, it was much longer; the Portuguese started extracting resources from Angola in the sixteenth century.

It is bitterly ironic and probably not accidental that much of the West's so-called "foreign aid" actually goes to cementing this choke hold. Every project that is funded by the World Bank in collaboration with local partners ends up as another point of control over local economies.

Don't feel complacent as you read this: Africa is just an extreme example of a general global problem. The economics of elitism that have kept Africa destitute for six generations also apply to the US and Europe. We could all be a lot wealthier, happier, and freer if governments kept to their role as arbitrator and regulator, and spent less time trying to interfere in markets to benefit their friends.

The wired Internet was, until recently, not very different.

As late as 2010, all of sub-Saharan Africa had only four lines to the outside world: the high-capacity fiber-optic cables that criss-cross the world's waters. The first of these was the SAT-3, which ran from Portugal around the West African coast, down to South Africa, then across the Indian Ocean to India. The others — TEAMs, Seacom, and EASSy — linked the East African coast to Sudan. EASSy was launched in 2003, and finally came on line in 2008. SAT-3 connects to nine African cities: Dakar, Abidjan, Accra, Cotonou, Lagos, Douala, Libreville, Cacuaco, and Melkbosstrand.

SAT-3 missed about twelve countries on the way, including both Congos. Still, it worked and in theory, the lucky citizens of those cities should have been able to get cheap access to that vast fiber-optic bandwidth ... except that these links to the outside world were built and owned by the same cartels of crooks that ran the ports: the ruling elites of African nations who had no interest in wealth generation unless it was for themselves and their families. The cost of wired Internet

when EASSy came on line in 2010 with its 4,720 gigabit capacity was about $5,000 to 10,000 for a 256 kilobit (not kilobyte) link.

That was about 50 times the price of a similar link in the US, which is not known for its competitive market. In relative terms, if you compare the per-capita gross domestic product (GDP) of Nigeria (one of the SAT-3 countries) against the US, there is a difference of 30 times, so that Internet price ticket is almost *1,500 times higher*.

Think about this for a minute as you surf the Web. Imagine being asked to pay $30,000 per month for an ADSL link that costs you $20 today, and you start to understand what kinds of hurdles ordinary Africans — who are very aware of what the Internet offers — have faced as they tried to get hooked into the modern world over the last decade.

Keep this in mind when you see a young black man who has walked and hitched in constant danger from West Africa across the Sahara, and has managed to cross the Mediterranean and make it to safety in Spain or Italy. Before sneering at one more unwanted economic refugee, ask yourself, "*What drives these young men to cross deserts and seas at terrible risk in pursuit of a life of inevitable marginalization in a hostile West?*" Perhaps part of it is simply the desperate need to get on line and become a citizen of the new world.

Lacking data, it's impossible to know how important getting on line is to young Africans. Speaking from personal experience, I'd place it about as high as getting an education, spouse, house, and family.

The only competition to expensive fixed Internet used to be the "very small aperture terminal" (VSAT) satellite system. In 2010, the cost of a VSAT package was about $8,500 for setup and equipment, and $5,000 for a 128KB (combined up and down bandwidth) link per month, surprisingly close to the SAT-3 costs. You could get VSAT if you were a government official or wealthy businessman. The common people had cybercafé clusters where several hundred people shared one VSAT link. And these were the lucky ones.

The elite was as possessive of its Internet privileges as of its Mercedes-Benzes and SUVs. It's not just that the state-owned telecom firms are monopolies that want to extort the market. It is that they are not even designed as profit-making entities. Rather, it's about patronage and selling favors. So whereas across the globe, the Internet brought freedom and enlightenment (as well as porn, identity theft, and viruses), in Africa it was poised to become one more tool to keep the power in the hands of the few. I use the past tense because magically (or naturally, if you are an optimistic believer in the human ability to solve even the hardest problems), the problem pretty much went away.

In 2011 and 2012, the West African Cable System (WACS) and ACE cables[23] each added 5,120 gigabits capacity (SAT-3 is 340 gigabits, by comparison). In 2013, SAex is adding 12,800 gigabits. Capacity is doubling every two years, finally, and cost gravity is biting. Given the lack of resistance from established cartels, intra-African Internet will be better and relatively cheaper than in the US and most of Europe within a decade or two.

What happened wasn't just improvements in cable technology. The old shortage wasn't a technical problem so much as a core feature of a centuries-old political system. WACS, ACE, and SAex became possible because the rules changed, and the iron stranglehold maintained by the old elites was broken. It happened during the first decade of this century, and it just took a few years for wired Internet to catch up.

How the monopoly of power in Africa died and freed a billion Africans to come on line is largely a hidden story. For outsiders, it was never clear why things were so bad to start with. For insiders, the changes feel inevitable and it's simply a question of catching up with the rest of the world.

---

23 http://www.oafrica.com/broadband/fibre-capacity-submarine-cables-and-african-internet-in-2022/

Yet for me, it makes an interesting and happy story with a strong positive message for the future. A continent of old, cynical, and murderous regimes that made poverty their business is transforming itself. This didn't happen by foreign pressure, nor by the hand of God, nor by the process of democracy, nor by building better institutions, nor by popular uprising. It happened simply thanks to the market and cost gravity, which shifted the balance of power away from the coastal elites and their foreign business partners.

The First Wave

What changed Africa was the mobile phone, at first, and then the smartphone.

Here are some interesting statistics for Africa, calculated by the International Telecommunication Union[24], or ITU, for the end of 2012:

- The number of fixed lines is 12 million, covering 1.4% of the population directly. This figure probably hasn't changed over the last 20 years. If you worked in Africa in the decades before 2000, you know how it worked. These phones were for official use, for wealthy businessmen, and for the elites. To make a phone call overseas, you had to reserve a slot in advance because there were so few international lines.
- Now, the figure for fixed Internet connections: 3 million connections, or 0.3% of the population. Of course, it's far easier to share an Internet connection than a phone, so I assume a lot of these are cybercafés in coastal cities. Still, this figure is shockingly low.
- There are, by contrast, 545 million mobile phone subscribers in Africa, which is an astonishing 64% of the population. And one in six of these are smartphones with mobile broadband Internet: a full 10% of the population. The number of phone subscribers has grown at 82% a year, compared to a global average of 40%.

24 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

This is a stunning development with deep social, economic, and political impact.

We can break it into two periods. The First Wave was roughly from 2000 to 2010 and brought a half-billion Africans the freedom to speak to each other across any distance. The Second Wave covers roughly 2010 to 2020, and will bring a billion Africans on line and into the global Internet.

I was talking to a trade union organizer in Lomé, Togo during the crest of the First Wave. She explained how now, if there was a strike at one mine, say in Namibia, news would spread to all mines owned by the firm, across the continent, and workers could shut down operations in fifty mines the next day.

The question is how that First Wave ever started. It certainly wasn't planned.

In 2000 or so, I was working in Lagos, Nigeria. We had European mobile phones, which did not work in Lagos. There was a network, which was excessively costly. Instead, we used long-range walkie-talkies, large chunky radios that we carried with us when we moved around. If we had an appointment in the afternoon, we'd spend a couple of hours in traffic jams, unable to tell our hosts we'd be late. Things happened very slowly.

In 1990, a decade earlier, New Zealand earned the honor of being the first country to use government-run auctions to allocate radio spectrum. It was a radical idea: a clever way to solicit big bribes from large firms in exchange for cartel control of a public resource while appearing "free market."

In 2000, many European countries held auctions to sell 3G space on the same basis. These auctions raised a huge amount of money and inspired several African governments to try the same. In January 2001, Nigeria auctioned off three GSM licenses and raised $285 million[25].

25 https://www.google.com/search?q=Nigeria+auctioned+off+three+GSM+licenses+and+raised+%24285+million

This was an enormous amount of money if you based your predictions off the number of fixed lines at the time: perhaps a few hundred thousand in all of Nigeria.

Before long, multicolored teams of South African engineers were filling Lagos' luxury hotels and planning how to cover the country with mobile phone base stations. I remember the buzz that the teams of young engineers brought to the city in 2001. Things were changing, finally. More or less the same happened across the entire African continent as every country organized its own lucrative spectrum auctions.

To build out the mobile phone networks, operators dug cables across every country, criss-crossing it with new, high-capacity fiber. In effect, the First Wave built the wiring that would allow the Second Wave. All it required was some upgrades of the cell towers — Chinese equipment is really so cheap — and new handsets.

The first handsets were very costly. They were the toys of the rich, which seemed to fit the old pattern where the rich got all the nice stuff and used it to improve their lives, while ordinary people became steadily poorer. Cost gravity was grinding away, and handsets got cheaper and cheaper until most families could afford them. In some poorer countries, like Togo, they were often third- or fourth-hand, battered old Nokias that had been sold in Europe, then Russia, then Nigeria, and then finally Togo.

The BBC wrote in 2007[26]:

> *With one in three adults carrying a cell phone in Kenya, mobile telephony is having an economic and social impact that is hard to grasp if you are used to living in a country with good roads, democracy, and the Internet. In five years, the number of mobiles in Kenya has grown from one million to 6.5 million — while the number of landlines remains at about 300,000, mostly in government offices.*

26 http://news.bbc.co.uk/2/hi/technology/6241603.stm

To poor people in remote areas, the mobile phone is much more useful than any conventional computer. It is portable, cheap, durable, has a long-lasting battery, and can do a lot. Once a mobile network exists, it can very rapidly scale up to the latest state of the art. And the lack of regulation — which enables corruption and stagnation in classic industries — creates space to innovate in the African mobile industry. In December 2005, *The Economist* wrote: "a call from a Somali mobile phone is generally cheaper and clearer than a call from anywhere else in Africa. The trick is the lack of regulation."

The First Wave did more than just bring phone calls and texts. The lack of regulation let African mobile phone operators invent services that would not be allowed in Europe, such as mobile banking. It's a simple concept: put money into your prepaid phone account, then send units to someone else, and you've made a transfer.

Arguably, African mobile phone credits were the first widely used virtual currency. You could pay for food, bribe a soldier on the other side of the country, buy a shirt, or send money to your nephew — all with no banking fees or conversion rates. Suddenly, a mobile phone became a debit card that worked at any distance. It's all the more significant because the conventional banking system was so out of reach for most people.

The Second Wave

Low-cost "Shenzen" electronics producers in China developed very fast production lines based on the open sharing of knowledge. That is, they publish the bill of materials (BOM) for their phones and other gadgets so that others can build modified versions. In return, those others also publish their BOMs. It's a nice remix that let the Shenzen firms shift very rapidly. Ironically, for a community based on trust, their main designs are imitations of market leaders, and Shenzen firms were infamous for making cheap and nasty iPhone clones.

Until 2009, these firms lacked decent operating software for their phones. Then Google bought Android and turned it into a realistic option for smartphones.

I'd argue that the developing world was only able to afford smartphones thanks to Android, which is based on Linux, the free software operating system. A mere 18 months after it was launched, Android already powered most of the smartphones coming from Asia, which were built by firms like HTC and Samsung.

For Africa, the combination of cheap Chinese handsets running a real Internet-capable mobile phone operating system was explosive. As I explained, the First Wave already built out and tested the infrastructure, so it was relatively easy to upgrade this to better and faster technologies. Cost gravity means new mobile broadband equipment is cheaper and better than older 2G equipment ever was.

I predict that by 2020, a billion Africans will be on the Internet thanks to mobile broadband and cheap smartphones running Android. We are heading towards a fully connected planet, in which 99% of those who can spell their own name will be computer-literate, on line 24/7, and tied into a global society that never sleeps, never stops thinking, never forgets, and never forgives.

Power to the People

Moving too rapidly for the old elites to respond with political crackdowns, African mobile operators have become a new power. Their networks are shifting to fast broadband. With their continent-wide wiring, they are the only people with the infrastructure to talk to those new WACS, ACE, and SAex cables.

The story isn't one of catching up with Europe and America, rather of leaping over it, much as Asia did when it unleashed mobile broadband. Tablets in schools, a phone in every pocket no matter how cheap the cloth, vast arrays of new digital products and services, and over time, the result is the emergence of economic giants. You don't in fact need super high-speed connections to the outside world, though

they are always welcome. What you need is a large internal market with the lowest possible friction, for it's there that the most activity happens.

During the Second Wave, local websites will spring up and digital societies will grow across Africa, creating fertile ground for an African digital economy. Cheap computers will raise a generation of connected children. African minds will solve the unique problems of African life, dependence on foreign aid will end, and poverty can be attacked as it has been across the world. Industrialization is not a necessary step on the road to development; digital society organically routes around models it does not find useful.

African entrepreneurs skilled in thin, fast, solar-powered networks and the software to make them work will start to sell their technology to other countries. Africa will become fully integrated into the global digital society and African parents will worry about porn and pedophiles, just like all mums and dads across the world.

This will transform Africa. The First and Second Waves have already done more to end poverty in Africa than five decades of IMF loans and World Bank grants, and I'm certain the trend is unstoppable. Even if occasional political interference and censorship throttles the Internet in some countries, Africa is huge and diverse, and competition among countries will ensure that things keep moving.

In summary, remoteness and isolation create poverty, and mobile phones are thus an obvious, compelling cure. They are cheap, accessible and usable by everyone, and a gateway to more sophisticated use of the Internet. Mobile phones are de-marginalizing the African majority.

The Asynchronous Society

Going digital and getting connected have already redesigned our lives and society. These changes are accelerating. In many ways, we've only started the process.

We now react to our social world in real-time, rather than relying on up-front planning and arrangements. Events used to take days to reach us and provoke a reaction. Now they take minutes. XKCD proposes[27] that reports of an earthquake across Twitter travel faster than the earthquake itself. We send an email instead of going to meet someone. We call home on our mobiles instead of being there at an agreed hour. We leave on trips without preparation, knowing that we can make things up as we go along. Hundreds or thousands of people simply waiting used to be a usual sight; now it exists only in airports and train stations when there are delays.

The appointment, previously the cornerstone of social life, has disappeared except as a business or medical formality. Scheduled meetings become more and more irritating as people learn to work asynchronously, each on their own clock. The synchronous institutions that still work by the clock — schools, government offices, older businesses — are legacies of the past, waiting to be reinvented by digital society and shuttered.

And the clock itself, a tool designed to get us to the right place at the right time, has become a strange anachronism. We stroll through our days, browsing on digital snacks, woken to action by emails, text messages, chats, tweets, and phone calls.

The event-driven lifestyle is so addictive — because it lets us be much more productive with much less effort — that a tool like the Blackberry (one of the first widely used smartphones) was nicknamed "Crackberry," and Facebook is called "Facecrack" by some. Take away our email and mobile phones and many of us would be left unable to function.

One surprising and good result of this is that many more people participate actively in society than ever before. It used to be hard to get involved beyond our physical world, that is, people we could meet face-to-face, places we could visit in person. Now it's trivially easy. The costs of publishing a work used to be a barrier to all except the

27 http://xkcd.com/723

lucky few. Being "published" used to be a sign of success. Today, there is no barrier except willpower and time. It means we have a lot more rubbish than ever before, and also a lot more genius. Overall, digital society is many orders of magnitude smarter and more interesting than the industrial society ever was.

Society used to be physical, based around where we lived and worked. Today, that is becoming less important, or at least more balanced. Our real cities no longer need to act as hubs of industry or business; they can instead become places to live in. And on line, we have created new virtual cities where people spend much of their lives making deep emotional ties that can last a lifetime.

It used to be very hard to find other people with the same interests as us. Now, a five-minute walk through the Internet finds friendly people around the globe who share our passions, no matter how esoteric. This often lets us turn passions into professions. More and more of us have built our own jobs doing things we deeply enjoy, thanks to the audience and market that the Internet brings us.

Freedom to choose one's own lifestyle has profound and positive psychological effects. Groups and organizations tend to domesticate their members by imposing more or less consistent styles of dress, language, diet, daily rhythms, space, emotion, and personal relationships. Aggressive groups, like cults, can break down a person's mind by forcing out all independence and replacing it with a synthetic groupthink. People who undergo such treatment become compliant and accept authority without question.

There is a whole dark science of turning intelligent individuals into accepting morons, simply through the manipulation of their social context. For more on this, see "Social Anti-Patterns" in "Spheres of Light".

Happily, in my experience, this process also works in reverse. When we can construct our own lives, we generally become happier, more productive, and more discerning. The easy dogmas of the past are broken down and a form of wisdom based on uncovering objective

truths takes their place. Like planting a forest tree by tree, it's a slow and almost invisible process and one that is, for me, absolutely key to understanding digital society. Freedom — which I define as the capacity to do interesting and useful things with other people — makes us better people. And digital society is truly a society of freedom.

When we spend a lot of time on line, we can know many more people than ever before. Our social networks used to be small, limited by our memories for names and faces. Today, our mobile phone and email contact lists are vast, and we can get to know hundreds — even thousands — of people on a first name basis.

So digital society is more connected than the old industrial society, and its members are more mobile, more interested, better informed, more critical and independent, and more able to react quickly to new events and opportunities. Planning and habit are redundant; instead, we keep our phones switched on, which beep when we get mail. Our social reaction time has dropped from weeks and days to minutes and seconds. This happens both on-line, with new communities springing up rapidly around new challenges and opportunities, and in the real world, with mobile crowds responding rapidly to events in the streets.

The Economic Quickening

> *Without protectionism, Germany sells the precision instruments to produce the optics, Japan designs the semiconductors, Taiwan fabs the chips and the Chinese assemble them with equipment bought from the West. Everyone benefits, is employed, and makes enough money to buy a $10 camera. — 1stworld, on Slashdot*

The economic impact of seven billion citizens joining digital society is vast and only just starting to be understood. Where this will take us is not clear. We can however already see the trends:

- All markets have more participants. In any given area of activity, the number of people who participate and compete has greatly increased.

- Rather than creating a race to the bottom, we see increasing specialization and diversity of suppliers, and lucrative new businesses constantly emerge.
- All markets are more equal. The tools available to even the smallest players give them real power within their markets.
- Smaller players are more educated and informed. The cost of getting information has fallen to near zero and today the size of larger players actively works against them.
- Competition has driven up efficiency and productivity and driven down costs in many markets.
- Industrial-age "capitalist" agreements such as the division of firms into owners, managers, and workers, have stopped working and are being replaced with far more egalitarian and flexible structures.
- Industrial-age market regulation is becoming less relevant as people choose more and more to rely on private law. For example, in the workplace, contracting has become a growing replacement for regulated employment.

The employee who is working for a large static firm is a zombie concept. The future belongs to the self-employed contractor who joins highly focused groups, some of which may be small companies, and most are simply "projects." The Internet hosts untold millions of such projects — an informal economy that must surely exceed the formal economy by at least an order of magnitude.

The reason is very simple: an employee who can work on one project at once is an order of magnitude less productive than a contractor who can share bandwidth with half a dozen projects. Not only can contractors specialize and thus be more efficient, they can also reuse their knowledge and skills over and over in different contexts. The cost of creating a new project has fallen to almost zero. The result is that the most skilled people are no longer content to work for established firms. It's so easy, fun, and potentially lucrative to work in small meritocracies that this lifestyle is today seen as a badge of success.

With flatter playing fields, more competition, and larger markets, we've seen a dramatic fall in the prices of all goods that have a significant digital aspect, and in their development, production, or distribution. Adam Smith wrote, one cold Scottish night in 1776 at the dawn of the Industrial Revolution: "*the wealth of nations comes from the division of labour, the pursuit of self-interest, and freedom of trade*."

He explained that economies and wealth are not cakes to be divided among the available hands and mouths. Instead, they are a product of how many of us there are, and how we organize ourselves. The cake fallacy is an error that even experienced economists sometimes make, equating, for instance, increased population with poverty, making the obvious — and wrong — reasoning that more people means less to go around.

Smith's ideal merit-driven free-trade markets have rarely appeared, because most politicians don't really care about prosperity except as a side effect of their drive to get and retain power. Digital society seems to come very close, at least until governments intervene with taxes, barriers, and censorship. There is a great temptation and a strong economic incentive for people with power to see markets as opportunities for self-enrichment. Markets organize themselves and fight back. And thus we get the start of political structures emerging from economic ones.

From Innocence to Authority

Some decades after social and economic changes, and no less disturbing to the old state of affairs, come political changes. The first years of the Internet were innocent. Commercial use of the Internet was banned and its political aspirations were childishly idealistic. Up until 1999 or so, most citizens of digital society who even considered the question would have answered that the Internet was going to define its own laws, that it would be free of the shackles of old laws, and that peace and prosperity would rule. Some people even tried to set up their own virtual countries.

Like many visions of the future, these early attempts were not inaccurate so much as set to a totally unrealistic time scale. Digital society, if it wanted freedom, would have to wrest it by force from the clenched claws of old power, just as every new society has had to do since the dawn of time. Those who set up virtual countries, complete with embassies and passports, were making a poetic statement, not trying seriously to get a seat at the UN (unless they were mad). People *were* naive enough in 1999 to invest real money in businesses like Napster that traded copyrighted materials in broad daylight, so to speak, under the assumption that the laws of the land did not apply to the Internet.

Around 2000, global content businesses — music, TV, cinema, news — looked at the Internet and saw a vast new world to conquer, sadly already squatted by pirates and hippies. The large and growing digital economy was consuming entire sections of the traditional economy. Some firms moved on line; very few got it right. Most firms just sent in the lobbyists and the lawyers.

Two great clashes perhaps define digital society's passing into adulthood. The first of these was the copyright debate, most notably the total lack of respect for conventional copyright law that people demonstrated by exchanging music, TV programs, and films in great numbers. The second was the patent debate, in which the industrial-age patent industry tried to move into software, successfully in the US and with partial success in Europe.

Both of these fights — which are widespread and ongoing — involve the basic definitions of "property" and the right of large firms to lobby governments into changing these definitions for their own benefit. Both are also typified by the politicization of digital society, as it finds that its road to freedom is blocked by old (copyright) laws or new (software patent) laws.

There are other fights as well, related to these. One is over the way the state is using digital technology to censor the Internet, to spy on its citizens, and to build up databases of every aspect of our lives.

Somehow, we don't mind too much if Google records every search we make and every site we visit. However, when our government records every phone call, email, search, and download, we get annoyed.

Unlike previous historical clashes between revolutionaries and reactionaries, digital society is highly knowledgeable, independently minded, and unafraid of confrontation and risk. It's also well connected and able to organize rapidly around new challenges. As business has started to lobby and litigate to try to keep control over the digital economy, digital society has reacted by organizing itself into more or less formal movements.

And like its businesses, digital society's political organizations are ferocious and can be exceptionally effective. In some of the civil society campaigns in which I used to be involved, we estimated that the professional lobbyists we were fighting had to spend as much as 1,000 times more money than we did to win. Well-organized volunteer activists are much more creative and accurate than professional lobbyists.

These are the main factors I see that affect political organization in digital society:

- Rapid dissemination of information to many people using tools like Twitter.
- Rapid analysis, discussion, and aggregation using Facebook or wikis.
- Cheap tools for bringing many people into virtual organizations.
- Ease of hooking into the existing news networks, which are desperate for news.
- Huge size of politically motivated communities that think globally and act locally.
- Increasing sophistication of these communities as they improve their organization and techniques.
- Increasing links between the digital economy and activist movements.

- Increasing links between old political parties and activist movements.

In some countries, digital society activism seems tied to certain political viewpoints: often a left-wing, collectivist point of view. More widely, digital society activism defines a new direction that is neither left nor right, sensing that industrial-era political parties, from left to right, are dinosaurs of a lost age and that twenty-first century politics revolve around new issues.

Chapter 2. Spheres of Light

The Culture grew, and grew faster than you could follow. In less than a generation it had started to build cities, impossibly beautiful spheres of fire and hope; massive, and yet gentler than the breeze.

In "Magic Machines", I described how the world has changed during recent decades. I explained how these changes threaten the economic and political structures that emerged from the Industrial Revolution and consolidated their hold over the world of the twentieth century. While society used to be based around cities built by steam and coal, it is now based around communities built by software and silicon. These communities are not passive. They are powerful and dynamic, and they challenge the economic and political structures of the old industrial world. We have witnessed Facebook and Twitter acting as platforms for real-world revolutions.

These on-line communities are largely self-organizing around problems of the day. They analyze information, share knowledge, debate strategies and tactics, and take decisions without explicit top-down leadership. They are "collective intelligences." It's not a new pattern in human society; indeed, the necessary instincts are deeply coded in our minds. Human society has always been a network of collective intelligences. It has never been so fluid, so large scale, so effective.

In this chapter, I'll explore how successful on-line communities work. More than that, I'll show how to build them, the shining digital cities of our future.

The Wisdom of Crowds

Niccolo Machiavelli observed, in "*Discourses on the First Decade of Titus Livius*" that:

"As for prudence and stability of purpose, I affirm that a

> *people is more prudent, more stable, and of better judgment than a prince. Nor is it without reason that the voice of the people has been likened to the voice of God; for we see that wide-spread beliefs fulfill themselves, and bring about marvelous results."*

In his book "The Wisdom of Crowds," James Surowiecki wrote, "*under the right circumstances, groups are remarkably intelligent, and are often smarter than the smartest people in them*." He noted that a collective intelligence usually produces better outcomes than a small group of experts, even if members of the crowd do not know all the facts or choose, individually, to act irrationally.

To put it another way, a group of random people will on average be smarter than a few experts. It's a counterintuitive thesis that mocks centuries of received wisdom. Experts in the field of human intelligence (sociologists, anthropologists, psychologists) did not embrace Surowiecki's opinions. He went further: adding more experts to an expert group will make it stupider, while adding laymen could make a stupid group smarter again. Like any recipe, it only works in specific circumstances.

I discovered Surowiecki when I started working on a reproducible recipe for building communities. His work immediately resonated with what I'd experienced, and it seemed testable. I had both the opportunity to apply it, and to experiment with enough communities to try to disprove it: the basis, thus, for real science.

Out of that work came a process for building smart, self-guiding, successful on-line communities that could beat expert groups every time. It is a discipline I named *Social Architecture*, which for a while let me call myself a "Social Architect." (Today, I'm a struggling writer, which sounds more romantic.)

Social Architecture, by analogy with conventional architecture, is the process and the product of planning, designing, and growing an on-line community. Social Architectures in the form of on-line communities are the cultural and political symbols and works of art of di-

gital society. The twenty-first century will be identified with its surviving Social Architectures.

As Social Architects, we participate in communities, we identify successful naturally occurring patterns or develop new patterns (which I call "tools"), and we apply these deliberately to our own projects. We apply psychology (our social instincts), economics (how we create common wealth through specialization and trade), politics (how we collect and share power), and technology (how we communicate). We continually adapt our toolkit based on new knowledge and experience. Our goal is to create on-line communities that can and do accurately solve the problems we identify, grow healthily, and survive on their own.

Successful on-line communities tend to be based on the contract of mutual benefit, whether implicit or explicit. That is, it is possible to build a billion dollar business based on volunteer labor, with every participant contributing for selfish reasons. Often, participants do not realize or care that they are part of a community. However, every action we take is economic. "Crowd sourcing" is the exploitation for profit of volunteer labor. And it only works when the crowd really wants to solve the problems you throw at it, or the ones it discovers.

Wiser and More Constant than a Prince

Machiavelli didn't explain or provide evidence for his observation. However the understanding that the collective will is accurate and honest — *vox populi, vox Dei* — pervades modern culture. It underpins our sometimes skeptical appreciation of democracy, and it justifies our demands for transparency and access to information. It is the basis for modern economies, based on free choice and free markets. It's the basis for at least one Humanist "religion"[28].

Surowiecki identified four elements necessary for a wise crowd[29]: diversity of opinion, independence of members from one another, de-

28 http://stallmanism.org/

29 https://en.wikipedia.org/wiki/Wisdom_of_crowds

centralization, and effective ways to aggregate opinions. He describes the ideal wise crowd as consisting of many independently minded individuals who are loosely connected, who are geographically and socially diverse, who are unemotional about their subject, who each have many sources of information, and who have some way to bring their individual judgments together into a collective decision.

According to Surowiecki, the wise crowd makes fast and accurate judgments, organizes itself to make the best use of resources, and cooperates without central authority. Some examples of wise crowds, such as Wikipedia, are extraordinarily successful despite intense and repeated criticism from naysayers and attacks from vandals and infiltrators. It's such a compelling proposition that we might wonder why we don't see more wise crowds. Indeed, why is the world filled with so much stupidity if it's so easy to be smart?

There are good explanations for the stupidity of many crowds, and I'll explore this later, in "Faceless Societies". Few people have tried to explain group stupidity in terms of collective wisdom. And without a clear understanding of function, how can we hope to understand dysfunction?

So the apparent failure of collective intelligence convinces many that this is just a fancy theory that fails in practice. And yet if we look at on-line communities, for example those that form around popular open source software projects like my company ZeroMQ[30], we see groups that look a lot like Surowiecki's wise crowds. While it may be hard to spot wise crowds in the physical world, they seem to be the dominant model on line. Through trial and error, digital society has rediscovered the principles of wise crowds and adopted them as its core operating principles.

Digital society's solution to the ancient problem of corrupt authority is elegant and successful. There are literally millions of communities, each backed by the authority of its founders. Citizens of digital society choose freely which authorities to respect and which to ignore.

30 http://zeromq.org

The core trick is to accept authority without giving it the "right to command."

Thus there is intense competition to develop fair authority that does not command, and instead enforces necessary rules. It is a deeply subversive truth. Generations that learn this model will refuse — to the point of death — to respect industrial society's model — enforced by iron curtains and armed border guards if needed — where the citizen literally belongs to the State.

Origins of Social Architecture

I've bet a lot of money on Social Architecture, and have made good profits. It comes close to hard social science, proven by years of reproducible experiments on living cases and studies of existing communities. It mixes psychology, economics, politics, technology, humanism, and optimism into something that I've found can make a lot of people pretty happy.

My journey into Social Architecture began in the late 1990's, when I began researching a book about how cults exploit our social instincts. Cults are not happy places, of course. However, humans are drawn to them because we're social animals who, over the last million years, have developed instincts for joining and conforming to groups in order to survive. It has become second nature for us to readily respect authority, conform, learn common languages, and adopt shared behavior. Cult groups brainwash their members by exploiting these instincts. They separate members from their families, eliminate privacy, flood them with jargon, create arbitrary rules, and punish and reward randomly.

In this way, cults can turn most ordinary people into unthinking followers who willingly empty their bank accounts, steal from their families, and work for years without pay. As a student watching the occasional friend disappear into the caverns of Scientology and other cults, this struck me as malignant and confusing. Later, when my

closest cousin dropped out and lost five years of his life to Scientology, it got personal.

Studying the Cult Information Centre (CIC) website[31], it struck me that these brainwashing techniques all have several things in common. First, they were all clearly focused on attacking individual thought and action, and destroying that which makes us strong. Second, they were reminiscent of environments in which I'd worked (big business often functions like a cult). Third, they all seemed reversible in that they could be flipped around to become positive patterns.

The last aspect is surprising. If a hammer breaks a window, you can hardly make a window stronger by reversing the hammer. Some examples make it clear. Take this technique from the CIC site: "*Peer Group Pressure — Suppressing doubt and resistance to new ideas by exploiting the need to belong*." The reverse is, by lowering the cost of joining and leaving the group, we encourage new ideas and criticism. Or, consider "*Removal of Privacy — Achieving loss of ability to evaluate logically by preventing private contemplation*." Its reverse is: give people private space and time to think, and they'll become better at thinking logically.

My conclusions persist. We survive by attaching to groups, following others, and trying to make sense of the world. Some groups work by domesticating and brutalizing us. Other groups work by giving us freedom and allowing us to be stronger, smarter, and more independent.

In 2000, the Internet had not yet become cheap enough for mass-market use, and open source communities were small and often regional, frequently focused around universities. Open source communities such as the Debian Foundation[32] still operated as classic not-for-profit organizations, as legal entities with boards, treasurers, and the like.

---

31 http://www.cultinformation.org.uk/question_what-is-mind-control.html

32 http://www.debian.org/doc/manuals/project-history/ch-detailed.en.html

In 2005, I joined a number of collaborative projects. On the one hand, I was involved with the FFII[33], working to stop software patents in Europe. We (the good guys) spoke in the European Parliament, debated with the European Patent Office (the bad guys), organized seminars, tabled amendments, got votes, and broadly, took part in the largest lobbying effort ever to hit Brussels.

On the other hand, I was developing open standards, starting with the Advanced Message Queuing Protocol (AMQP). The contrast between the cultures of these organizations was sharp. The FFII was a group of crazy volunteers, creative beyond belief, and filled with hard cold determination to stop SAP, Siemens, Microsoft, and Nokia (more bad guys) from changing European law to legalize the gray market in patents on software. The AMQP workgroup included banks and large software firms, who turned out to be crazy in a different and less enjoyable way.

With insanity surrounding me on all sides, research on social instincts and cult techniques suddenly seemed relevant again. With my friends in the FFII, we launched campaign after campaign. Websites, petitions, email lists, conferences ... it never stopped. Most of our campaigns failed to get any real scale though a few did. Above all, for about three years, we experimented, and we collected results.

We learned two broad things. First, a cult is the flipside of a wise crowd. The cult patterns seemed accurate, and I watched people applying the cult model to others over and over. Any intense group, family, business, or team starts to resemble a cult, in little or larger ways. It's a matter of degree. However, as soon as you spend your free time on someone else's project, you are essentially starting to slide down that slope. I watched as entire groups went off the rails, unable to think straight or produce accurate results. There was a straight causal effect: as the group became more cult-like, they became more useless.

33 http://ffii.org

The second thing is that just reversing the cult techniques isn't enough. It does make a good start to promote individual strength and creativity, yet that is not the same as building a solid community. For that, you need more explicit patterns. Define a powerful mission to attract newcomers. Make it really easy for people to get involved. Embrace argument and conflict; it's where good ideas come from. Delegate systematically, and create competition. Work with volunteers more than employees. Get diversity and scale. Make people own the work; don't let the work own the people.

It is of course much cheaper and faster to do large-scale experiments with people on line than in the real world. To prove or disprove a recipe for building a community, all you have to do is create a space, define some rules for play, announce it to the world, and sit back and watch.

My largest and most successful experiment to date, which I'll refer to often in this chapter, is the ZeroMQ software community[34]. It has grown from a team in a Slovak cellar to a global community, and is used by thousands of organizations. Above all, ZeroMQ is entirely built and steered by its community: over a hundred contributors to the core library, and a hundred other projects around that.

The Toolbox

In my Social Architect's toolbox, I have 20 tools, each covering one aspect of a community or group. These tools work in two ways. First, you can use them to measure an existing community, giving a rating of zero or more. Second, you can use them when you design a community, to help you focus your effort on where it will be most useful.

- *Strong mission* — the stated reason for the group's existence
- *Free entry* — how easy it is for people to join the group
- *Transparency* — how openly and publicly decisions are made
- *Free contributors* — how far people are paid to contribute

34 http://zeromq.org

- *Full remixability* — how far contributors can remix each others' work
- *Strong protocols* — how well the rules are written
- *Fair authority* — how well the rules are enforced
- *Non-tribalism* — how far the group claims to own its participants
- *Self-organization* — how far individuals can assign their own tasks
- *Tolerance* — how the group embraces conflicts
- *Measurable success* — how well the group can measure its progress
- *High scoring* — how the group rewards its participants
- *Decentralization* — how widely the group is spread out
- *Free workspaces* — how easy it is to create new projects
- *Smooth learning* — how easy it is to get started and keep learning
- *Regular structure* — how regular and predictable the overall structure is
- *Positivity* — how far the group is driven by positive goals
- *Sense of humor* — how seriously the group takes itself
- *Minimalism* — how much excess work the group does
- *Sane funding* — how the group survives economically

We will look at these tools one by one and see how they work in various communities. First, some general advice about building a community. Be brutally honest with yourself and with others. Your biggest challenge is overcoming your own prejudices and biases, and then those of everyone you work with.

Whatever toolkit I can provide you with, you'll want to adapt and extend it for your own needs. Social Architecture is still a very young science and many of my tools will be too complex, or incomplete. Here's the best way I know to do that:

- *Consume your own product.* If you are not a fanatical user of whatever your group is making, you are half-blind. I learned this when working for Nigerian Breweries in the 1990's: by enjoying

beer, I learned to appreciate the business of selling beer so much better.

- *Practice and repeat.* It is cheap to experiment, and failure is healthy. By definition, if you start a project and it fails, no one notices. So start many projects and change or fix your tools if they don't work.
- *Do first-line support.* All communities have a place where newcomers arrive and ask questions. Be there, observe how new visitors get lost, what mistakes they make, and improve your designs accordingly. Perhaps the mission confuses them. Or maybe the structures are confusing. A good designer sympathizes with his users, feels their pain, and works to relieve it.
- *Release early, release often.* This is a mantra from free software communities. It's accurate. You want to do your design work in the open, and get critical feedback as early as possible. In ZeroMQ, we release every patch as it happens.
- *Learn and teach all the time.* Teaching gives you perspective, and learning lets you pick up new tools over time. Social Architecture is a young craft, and though the basics are solidly anchored in human psychology, there are still many unknowns.

Strong Mission

The starting point for any community is a stated mission. The mission defines the goals that we can all agree on in advance, before we join the project. It's like the title of a website or the slogan for a movie. For instance, Reddit's title is: "the front page of the Internet," an ambitious mission that it nonetheless achieved. Facebook's slogan is: "helps you connect and share with the people in your life."

TIP: Use your mission as a slogan, on your website, marketing, presentations, and so on. If you are investing money in your community, you may want to trademark the mission statement.

Without a clear mission, an on-line community won't grow. A group of friends who start a project may agree what they want to do,

yet anyone new coming on board has to guess what they had in mind. People will guess wrong, and will change their minds over time. This leads to confusion, disagreement, and disappointment as people find that their hard work was wasted because the rest of the group headed off in a different direction.

A good mission saunters past "sane" and steps into "you cannot be serious!" Wikipedia's mission, "the free encyclopedia that anyone can edit"[35] is a good example. It was, initially, a goal that everyone, except a few idealists, found impossible and crazy. Those idealists were precisely who Wikipedia needed to get on board on day one. Impossible missions attract the right kind of people for a young project.

TIP: Change your mission as your community matures. At first, you will want to attract idealists and pioneers, then the leading edge, and then early adopters, the mass market, and finally, the late adopters. Each of these groups wants different things. Understand that, and tune your mission to suit.

To formulate a good mission, think in terms of the single main problem your project is solving. Reddit, for instance, is solving the problem of how to get the news off an Internet with far too many interesting sources of information. Its "front page" represents the digital newspaper of the twenty-first century. Wikipedia is solving the problem of how to collect knowledge from the minds of billions. "Anyone can edit" represents *vox populi, vox Dei*, the understanding that truth, if it exists, comes only from the minds of many.

TIP: When proposing action, small or large, try always to start by identifying the problems you want to solve. Only when you have a clear and real problem on which everyone can agree, move to discussing solutions. A solution for an assumed problem is like a group without a clear mission.

You may have multiple missions, by accident or deliberately. This can be traumatic if the missions pull in different directions. For ex-

35 https://en.wikipedia.org/wiki/Main_Page

ample, growing a group larger may require subsidies, which conflicts with making profits. If Wikipedia became a for-profit entity with advertising and an expensive tranche of managers, do you think its community would grow or shrink?

For ZeroMQ, our stated mission was "Fastest. Messaging. Ever." This is a nice, and nearly impossible answer to a problem we could all agree on: namely, the slow, bloated technology available at that time. However, my co-founder Martin and I had conflicting goals. He wanted to build the best software possible, while I wanted to build the largest community possible. As the user base grew, his dramatic changes, which broke existing applications, caused increasing pain.

In that case, we were able to make everyone happy (Martin went off to build a new library called "Nano"). However if you cannot resolve mission conflicts, it can damage the project severely. Projects can survive a lot of arguments, however fights between founders are traumatic.

TIP: If the founders agree that "success" is defined as "having the most participants possible," it can help in keeping your focus over the years. It also makes it easy to measure your success as you grow.

Free Entry

Once you have agreed on your mission, you need to test this against the real world. That is, you have to make a minimal yet plausible answer to the problem you identified. I call this a "seed." With the seed, you have two main goals. First, to start to collect idealists and pioneers (basically, anyone mad enough to trust you) into a community. Second, to prove or disprove your mission.

Projects fail for many reasons. A major cause of failure is that the original idea or mission wasn't as amazing as people felt. Failure is fine, even excellent, unless it costs years of your life. Making a seed and showing it to a few people isn't enough because most people won't be really critical. They feel it's hurtful. However, ask people to

invest even a few hours of their time in making it better, and if they don't say "yes," you know how they really feel.

TIP: Build a "seed" product in public view and encourage others to get involved from the start. If people do get involved, promote them rapidly. If they don't, treat that as a sign your mission may be wrong. Use the seed product to build the community.

Once people agree to help you, they need somewhere to work together. You need a "collaboration platform." My two favorites are Wikidot[36] for knowledge communities, and GitHub[37] for software projects. The platform has to be free to use. It has to be easy to learn and work with. Your seed project has to be visible to anonymous visitors. It has to work for anyone no matter his or her age, gender, education, or physical location.

All this makes it possible for interesting strangers to walk up and look at your work and, if they like it and feel challenged by it, get involved little by little. You want to be working on your seed in public view, and talking about your new project, from the very start. This means people can make suggestions, and feel involved, from day one.

If we, as founders of a group, choose those we work with, we're building in "selection bias." It is much easier to work with those nice, smart people who agree with us, than the idiots and critics who disagree. And when you agree with me, you just confirm all of my biases and assumptions and I know from experience that those can be wrong in the most amazing ways.

Over time, collecting people who share the same broken assumptions and biases can kill a project. For example, when making software protocols, the requirements for large firms can be very different from those for small open source teams. So if a protocol committee is built entirely out of large firms, what they make will be indigestible by the mass of the market.

---

36 http://wikidot.com

37 http://github.com

The answer is free entry to anyone who is interested, no matter how different or apparently crazy their perspectives. This gives us, potentially, that broad and diverse community which is the raw material for a wise crowd. In ZeroMQ, we never turn away anyone who wants to contribute. I pull people in, even if their contributions are poor or incorrect. The community is more important than the product.

When the community has matured around the seed product, they will want to build a second generation of it. As Social Architect, your goal is to time and guide this properly so that you can use the wise crowd to help design the "real" product. It's possible that around this point you will want to find a good domain name and make a "proper" website.

TIP: If people are not joining in your seed, don't continue working on it. Instead, discover what's stopping them from joining and fix that. Start again from scratch if necessary. Don't prematurely kill seeds; it can take time for people to appreciate what you are trying to do.

Transparency

Transparency is very important to get rapid criticism of ideas and work in progress. If a few people in a team go off and work on something together for some time — a few days seems harmless, a few weeks is not — then what they make can be presented to the group as a *fait accompli*. When one person does that, the group can just shrug it off. When two or more people do that, it becomes much harder to back off from bad ideas. Secrecy and incompetence seem bound together. Groups that work in secret do not achieve wisdom.

TIP: When one person does something in a dark corner, that's an experiment. When two or more people do something in a dark corner, that's a conspiracy.

With ZeroMQ, it took us some years to come to a really open and transparent situation. Before that, the core contributors mostly worked in secret, publishing their work when they felt it was ready for

public view. By the time they did that, it was very hard for the rest of the community to say "no." And often the work was off course, a brilliant solution to a problem no one really cared about. In the end, we explicitly banned this kind of thing.

It is ironic that secrets seem essential to certain business models. Profits often come from the ignorance of customers. Most profit-making businesses, even large communities like Twitter, depend on a strict division between "them" and "us." However, digital society grows best by putting scale before profits, and by treating all ignorance as a problem to solve. If your clients are ignorant of your internal thought processes, then you will be ignorant of where those processes are wrong.

Free Contributors

Money is a funny thing. Too little, and the community starves (I'll return to this later). Too much, and it rots. It is important to understand why each contributor is there at all. *What are their economic motives?* Even in a volunteer community, every person is there for self-interested reasons.

In ZeroMQ, we originally started with a small paid team and moved after two years to a community of volunteers through the pragmatic — if not very gentle — tactic of running out of money and having to fire the developers. A few disappeared to other jobs, some came back as contributors, and the project became more exciting and fun than before. People contribute to ZeroMQ because they need it in their own projects, and if they spend a little time making it better, that can earn them or save them many times more.

When you work for someone else, you will make what he or she wants. When you work for yourself, you will make what you need. It is so very different. People with money yet no skill or taste are the riff-raff of society. We despise paid contributors to Wikipedia, paid bloggers, and paid moderators on Reddit, because we know that the opin-

ions they express are almost by definition false. Would a blogger paid by Hollywood criticize the new summer blockbuster?

I've nothing against employees. However, if you are aiming for the largest, most successful community, you want contributors who are there for honest, transparent reasons. If a filmmaker comes to Reddit to discuss his work, that is fantastic. If his marketing staff come to downvote critical comments, that is despicable.

TIP: One free contributor is worth 10 paid contributors.

Full Remixability

A group needs a lot of agreements for working together. I call these "protocols." Perhaps the most important one for any creative community is remixability. Whether it's music, art, images, video, comments, software, or wiki pages, the following question *will* arise: "What is the copyright license on this work, and how does that affect the community?"

Broadly, there are three types of agreement for copyright:

1. A "locked down" license that does not allow remixing. This is the old way of working, and still the dominant model in for-profit work.
2. A "free to take" license that allows one-way remixing. This is the dominant model for many open source software communities.
3. A "share-alike" license that enforces two-way remixing. This is the dominant model for free software communities like ZeroMQ, and for many artistic communities (though it may be an unwritten agreement).

Users prefer the "free to take" model because it lets them use the content in any way they like without reciprocity. Imagine a DJ who releases a popular track under the "free to take" model. Then a company makes a remix and uses that for an advert. And that remix will be locked down. Now, the DJ cannot remix that new work, and may find himself unable even to play the remix.

Communities, however, work better with the third model because it converts users into contributors. With a share-alike license, the DJ would be able to take the remix, mix that further, and turn it into a dance club success. Knowledge and ideas flow in all directions, rather than leaking out of the community into closed dead-ends. The shift is powerful, especially for those of us building communities with a minimal budget. If you're a large firm putting a lot of money into a community, the "free to take" model can work better.

TIP: If every contributor owns their specific contributions, and you use a share-alike license, you don't need copyright assignments or re-licensing from contributors.

Strong Protocols

Good protocols let strangers collaborate without up-front agreement. They resolve destructive conflict, and turn it into valuable competition. The insight that lets anarchists join wise crowds as happily as anyone is that the crowd can develop its own rules. Typically, these rules govern remixing, identity, ranking, and so on. No matter what their form, good rules are simple, clear, explicitly written down, and agreed upon by all.

If you're building a software project, you might take an existing rulebook, like the C4.1 protocol[38] we built for ZeroMQ. Otherwise, you can start with a minimal rulebook and grow it over time as you see what problems hit the community. This is, for example, how the Wikipedia rulebook[39] grew up.

Some rules must be established very early (such as licenses for contributions). Others can be developed when needed (such as processes for resolving conflicts). Complex, pointless, or unwritten rules are toxic to groups. They create space for argument, confuse people, and make it expensive to join or leave a group.

---

38 http://rfc.zeromq.org/spec:22

39 http://simple.wikipedia.org/wiki/Wikipedia:Rules

TIP: Write your rules very carefully, starting with choosing a license for content, and measure how much they help people. Change them over time as you need to.

Fair Authority

Without authority, rules have no strength. The community founders and main contributors are its de facto authority. If they abuse this position, they lose contributors and the project dies or gets forked under different rules. Authority needs to be scalable (that is, work with any size of group) and transferable as the group grows and changes over time.

While we need authority to build a flat playing field, many groups use authority as a way of controlling members, keeping them in the group, and making them conform. A favorite cult technique is to randomly punish and reward people so they become confused and stop questioning authority.

TIP: Promote the most active contributors into positions of authority, and do this rapidly. You have a short window for promoting new contributors before they disappear to other projects.

You have to be a part of your community, and you must follow your own rules. If you find yourself breaking, or wanting to break, your own rules, they are faulty and need fixing.

In the ZeroMQ community, we've had fights over who had the right to define the rules, and in the end it came to the trademark and domain name. The person or company who owns the project name is the ultimate authority for the rules. If they're nuts, the project will die.

TIP: If you are investing money in the community, then consider taking a US trademark so that you can stop people from making similarly-named imitations that don't follow your processes. It costs about $750.

Non-Tribalism

Membership must be a badge to collect, not an identity. As Mr. Spock so often observed, emotions are not logical. Some groups are driven by logical purpose, and others by more emotional factors such as peer pressure, the herd instinct, and even collective hysteria. The main factor seems to be the relationship between the group and its members. We can quantify this: *Do members "belong exclusively" to the group?* Exclusive membership means putting the group's existence above its work. Exclusive membership ends in conflict with other groups.

TIP: Stay away from formal membership models, especially those that try to convert people to belonging to the group. Allow anonymous or unidentified participation. Encourage people to create their own competing projects as spaces to experiment and learn.

Industrial-age groups, like cults, specialize in owning their members. An employee belongs to his or her company. In some cases, even ideas you have in the shower are property of your employer. And when a group owns its members, it motivates them with emotions like fear, hate, jealousy, and anger, instead of purposeful logic. The threat of expulsion is widely used to get people to conform. "Do what I say or I'll fire you!"

TIP: To measure how tribal a group is, just start a competing project. If the response is negative and emotional, the group is tribal. A sane group will applaud its new competitors.

Self-Organization

Some people like to be told what to do. The best contributors and teams choose their own tasks. A successful community recognizes problems and organizes itself to solve them. Further, it does that faster and more accurately than any top-down management structure. This means the community should accept contributions in any area, without limit.

Top-down task assignment is an anti-pattern with many weaknesses. It makes it impossible for individuals to act when they recognize new problems. It creates fiefdoms where work and the necessary resources belong to specific people. It creates long communication chains that can't react rapidly. It requires layers of managers just to connect decision-makers with those doing the work.

TIP: Write rules to raise the quality of work and to explicitly allow anyone to work on anything they find interesting.

In ZeroMQ, we removed all assigned tasks from the community. For example, we don't accept feature requests. If someone wants a feature, they either send us a patch, or offer someone money to make the change, or they wait. This means people only make changes they really need to make.

TIP: Communities need power hierarchies. However, they should be fluid and heavily delegated. That is, choose the people you work with, and let them choose the people they work with. Power structures are like liquid cement; they harden and stop people from moving around as they need to. Any structure defends itself.

Tolerance

A diverse group has conflicting opinions, and a healthy group has to embrace and digest these conflicts. Critics, iconoclasts, vandals, spies, and trolls keep a group on its toes. They can be a catalyst for others to stay involved. Wikipedia thrives thanks to, not in spite of, those who click Edit to make a mess of articles.

It's a classic anti-pattern to suppress minority ideas and views on the basis that they are "dangerous." This inevitably means suppressing new ideas as well. The logic is usually that group coherence is more important than diversity. What then happens is that mistakes aren't challenged, and get solidified into policy. In fact, the group can be more important than the results, if it is diverse and open to arguments. This is a difficult lesson that applies to broad society as well: there are no dangerous opinions, only dangerous responses.

The way communities deal with trolls and vandals is one thing. To deal with fundamental differences in viewpoint is something else. I've said before that conflicting missions can be a problem. The best answer I know is to turn the conflict into competition.

In software, we do this by making standards that teams can build on. Take for example the HTTP standard that powers the web. Any team can build a web server or a web browser. This lets teams compete. So Google's Chrome browser emerged as a lightweight, faster alternative to Firefox, which was getting bloated and slow. Then, the Firefox team took performance seriously, and now Firefox is faster than Chrome.

TIP: When there is an interesting problem, try to get multiple teams competing to solve it. Competition is great fun and can produce better answers than monopolized problems. You can even explicitly create competitions with prizes for the best solutions.

Measurable Success

It's all very well to try to turn conflict into competition. However, you also need to provide teams with a way to know how well they are doing. The best tools, like GitHub, show you precisely how many people are watching or have "starred" or "forked" a particular project (revealing different levels of interest and commitment).

The Web, of course, has always been obsessed with "hits" and traffic analysis, which show exactly how popular a specific site or page is. This makes it very easy to measure success of on-line projects. In the old industrial-era business, teams get their feedback from their bosses. This turns into an exercise in power: you'll be scored higher for compliance than for accuracy. Making your bosses happy so they give you a pay raise is not healthy.

TIP: If your platform does not support it directly, find ways to tell contributors how well their projects are doing.

High Scoring

There are many reasons why people contribute to communities. An overriding motivation is to be admired for success. That can be as an individual, or as part of a team. Success is relative so we need metrics, some high score that people can see and track.

In the ZeroMQ community, we don't emphasize high scoring much, though contributors do get more love when they contribute more. It goes on their permanent record. Contributing to ZeroMQ can land you a good job.

Reddit, like many sites, uses "karma" that shows how many votes a profile got for its posts and submissions. It works pretty well. Some sites don't show all karma in order to stop people playing the system to just get a higher score. Some sites, like StackOverflow, have taken "gamification" to an extreme level, with badges, high scores, achievements, and so on. I think this is manipulative and distorts the mission of the community. People should be contributing because they need the project to succeed, not to earn toy points.

Having said that, social credit — making groups of strangers happy — is enormously satisfying and does not pollute the planet. Industrial society focuses on material rewards (higher salary, larger house, nicer car) tied into a hierarchical structure. It is effective because we all like wealth, or we have a daddy complex; whatever the reason, wanting to make the boss happy means taking fewer risks.

TIP: When there is something that people are asking for, and you don't know how to do it yourself, announce publicly that it is "impossible." Or, propose a solution that is so awkward and hopeless that it annoys real experts into stepping up.

Decentralization

In his book, Surowiecki explained how the Columbia Space Shuttle disaster was caused by a hierarchical NASA management bureaucracy that ignored the knowledge of low-level engineers. If a group is de-

centralized, its members are more independent, they receive more diverse inputs, and they are also likely to be more diverse from the start.

If a group is geographically concentrated, it becomes homogenized, where all members get pretty much the same inputs and triggers. Close proximity also lets a minority dominate the mindset of the group and quash unorthodox ideas. It lets them literally bully or bluff the majority into compliance. Insisting that all members of a group sit in the same office, department, or building is an old anti-pattern that is hard to break. There's a reason cults have compounds.

TIP: Do you need meetings to get work done as a group? This is a sign that you have deeper problems in how you work together. You are excluding people who are not physically close by.

It can be hard to move away from the old discuss-then-execute model of working together. Certainly it's easier if you are building groups from scratch than if you are trying to change existing groups.

Free Workspaces

A community needs space in which to grow. In Internet terms, this is typically a website or collection of sites, and related structures like email lists, blogs, and so on. We've seen that it's become very cheap, or free, to create "space" in digital society. The question is, can individuals create their own spaces within the community? If so, they will invest more in the collective project.

The freedom to create structure annoys people who feel that it creates chaos and disorder. However, if you use regular structures (see the next section), there's no real cost to participants. What is toxic is *speculatively* creating structure based on the assumption that people might need it. When I took charge of the FFII association in 2005, the previous president had created several hundred email lists, representing all the projects *he* felt people should be working on. It didn't fit how people wanted to organize, and it was very hard to delete these lists and create the ones we actually needed.

Of course, industrial-era groups do assign work, and assign the resources to carry it out. Any new infrastructure — such as a website, email list, or wiki — requires approval and a decision. It might even need legal review due to copyright and patent concerns. The cost is high, so people are reluctant to take the risk. Thus, they don't experiment and often work with one hand tied behind their backs.

In the ZeroMQ software community, it takes a single click to create a new project. In Wikipedia, you can create a new page simply by clicking "create this page." Both projects have mechanisms to stop random garbage from accumulating. Wikipedia purges new pages quite aggressively. ZeroMQ has an extra manual step to bring a new project into the official community organization.

TIP: Make it absolutely simple for logged-in users to create new projects. If projects are organized per user, you don't need to worry about junk. If they're in a shared space, you may need tools to purge junk and abandoned projects.

Regular Structure

As a community grows larger, it can become harder to navigate. If you make a single, ever-growing project, this becomes more and more complex over time, consisting mainly of special cases. Think of a medieval castle. This problem is particularly bad in projects built by larger firms that seem to lack a sense of cost.

Complexity turns people away because it's so difficult to learn. The solution is to use very regular structures that you can learn once and then predict many times. Not any structure will do. We seem bad at learning structures deeper than three or four levels. However, we're happy to explore very wide structures with thousands or millions of boxes if those boxes correspond to separate units of work, or projects. Think of a city.

The successful on-line communities are cities, not castles. Wikipedia consists of a few language-specific wikis, each broken into millions of pages (the projects), each structured into sections, discussion, history,

footnotes, and so on. Several people may be working on a page at once, and one person may be slowly editing or caring for dozens or hundreds of pages.

GitHub manages millions of software repositories or "repos," grouped under user profiles or organizations, and each broken into some further structure (source files, documentation, etc.) that usually depends on the language (Java repos use one style, C repos use another, and so on). One repo may have a handful of contributors, and people will work on a few to a dozen repos. The ZeroMQ community consists of an organization that contains a growing number of projects.

TIP: Design your community as a searchable city of projects, where anyone can start a new project, projects represent perhaps a dozen people's work, and all have familiar structure, as much as possible.

Businesses love their castles, which inevitably describe Important People, not projects, and certainly not the major business problems. Their organizations are huge and irregular. There's no way to understand them except by memorizing them in detail. Then again, you can't simply move around the castle, so there's little benefit in learning its layout.

Smooth Learning

When ZeroMQ started, it was one project with a single "README" page. Today, it's a hundred or so smaller projects, each with its own documentation, community, and process. To get into a mature project can be painful. As I've said, regular structures are essential. More than that, you need a fairly specific learning curve that goes from simple to hard as people progress from idle passer-by to expert contributor.

Think of your community as a video game with levels that become increasingly difficult, and have bigger and bigger payoffs. People will play "up to their level." If you can do this right, you attract the most

people. If you do this wrong, you'll bore experts by making it too easy, or you'll turn off others by making it too hard to get started.

TIP: Use classic training tools — presentations, videos, answers to frequently asked questions (FAQs), tutorials — to get people started. It helps if you are part of the community so you can see what kinds of questions people ask when they start.

Many existing organizations make no effort to create a smooth curve. Everything starts complex and stays there. To participate, you might need weeks of training. It's inefficient, frustrating, and expensive to scale.

Positivity

It's tempting to try to provoke people into joining a group by being aggressive. After all, many people enjoy a good heated argument, especially when they feel they're right. Some groups thrive on being quite hostile and negative towards other groups, particularly if there is some history involved. The tone you set as founder will last a long time. If you promote your community by attacking competitors, you will attract people of a certain mindset, and the culture will spread. Sooner or later, the negativity will turn inwards and can be very damaging for the community.

TIP: When you talk about people, products, or organizations, be polite and stay balanced. When you promote your product or community, talk about the problems you solve, not how you are better than your competitors.

It's better in my experience to set a positive tone from the start. Competitors are good because they give you resistance. Copycats are good, because they prove your market is a real one. Trolls and vandals are good, because they give sincere people an extra chance to prove their value. And so on. It seems like hard work to look for a positive outcome for every event. However, it's really just a mindset.

TIP: Welcome everyone, and only intervene when there are irredeemable troublemakers. It's a small minority that really can't find a

place in an open, diverse community. You can ask such people to leave and, if necessary, ban them.

A positive culture is more tolerant and reduces emotions and arguments. It also makes it easier to experiment, make mistakes, and self-criticize, and all these help a community think through difficult problems.

Sense of Humor

Have you ever wondered why humans have an instinct for humor, and why people who never laugh seem odd or unfriendly? My theory is that we evolved humor as a way of defusing conflict (which has obvious survival value). People don't punch the joker unless the joke is old or badly told. More subtly, humor defuses tribalism and emotion, and lets people work together even when they have huge differences. A shared joke creates strong bonds because it proves the intersection of minds. Humor is an essential part of a community and reduces stress.

TIP: The more serious your message, the more you need humor. In my ZeroMQ book, I wrote a lot of silly nonsense mixed with the heavy technical explanations. Most people enjoyed and appreciated this.

If it weren't for alcohol, the grim-faced industrial economy would barely ever laugh. It takes itself so seriously. The lack of humor in an organization is a sure sign that everyone there is fundamentally miserable. Worse, it makes the group vulnerable to conflict and fracture.

Minimalism

You make a racing car faster by removing weight, not by adding power. You can make your community lighter, faster, and more agile by being dogmatically minimalist about the work you do. Though it sounds lazy, it's often harder to *not* do something that seems fun than to just go ahead and do it.

The general rule is *do the absolute minimum that probably works*. Then invest more only as people start to use your work and complain.

Never invest more than the absolute minimum you need to get a "bite" from users. This applies to your seed product as well as every change you make. User feedback — more than your own vision — is the best guide for where to make further investments.

TIP: Perfection precludes participation. Releasing buggy, half-finished work is an excellent way to provoke people into contributing. Though it can be hard for big egos to accept, flaws are usually more attractive to contributors than perfection, which attracts users.

The culture of minimalism can, and should, extend to your community itself. In the past, we used to make legal entities for serious projects so there would be a place to hold copyrights, trademarks, and money. However, legal entities are expensive and time-consuming to manage. Tax reporting by itself can be an unbearable burden.

One of my communities, Digistan[40], was designed, grown, and did its work (building a new generation of legal templates and political arguments for open standards) in about six months. All of our ZeroMQ protocols are based on the Digistan work. The Open Web Foundation[41] — solving the same problem — spent two years simply building a legal entity, defining bylaws, and electing officers.

Sane Funding

If there's not enough money, a community will starve. If there's too much, it will, as I've said, rot. It is a delicate balance. We can motivate people with money up to a certain degree. After that, only sociopaths respond proportionally. This is a flaw in the naive "more money is always good" theory of capitalism. In my business, it's always been those I paid best who turned out to be the most treacherous.

The first thing is to reduce your costs by not setting up legal entities, offices, and staff unless you really need them. Not only will these eat any funding you might have, they will work against you as you try

40 http://www.digistan.org

41 https://en.wikipedia.org/wiki/Open_Web_Foundation

to build a pure on-line community. Secondly, invest your time and money in the community minimally when you see that there's no choice. It could be taking a trademark, paying for hosting services, or doing some particularly difficult work no one else is able to undertake. Finally, watch out for individuals who take on too much risk without adequate reward — they can be vulnerable to burnout, something I'll talk about in the next section.

TIP: Every time you find it necessary to spend money on the community, ask if you could have found a way to get others to help instead.

Sidebars

In the previous section, I examined my toolbox for building on-line communities. Now I'll look at few other key ideas that are worth knowing about.

The Market Curve

The market curve[42] is a well-known theory of marketing that is less known in engineering and community building. However it's important to understanding how communities develop over time. In the classic market curve, a new technology, idea, or product enters the market as a wave, starting with ice-breaking enthusiasts and pioneers, then the early adopters, then the mass market, then the late adopters, and finally the skeptics.

Each of these groups has different motivations for coming to a project, joining in, and eventually, leaving. If we take an exciting new technology like ZeroMQ, we can explore this and understand how it works:

- When the project is young and experimental, it attracts pundits and researchers whose business is new stuff, in general. These people need to know why the project is different from what exists, what its goals are, and why it is exciting. They will never use it, nor

42 https://www.google.com/search?q=marketing+curve

will they become contributors. They are your evangelists. They often lose interest rapidly.

- When you have a seed product, it attracts pioneers. These are hard-core hackers who want the latest stuff and don't care about documentation, marketing, or tutorials. They're very good at managing the risk of new things. These are your first wave of contributors. Often they are building frameworks for other developers.
- When you have a real, usable product, it attracts early adopters. These are people making real products yet who are good at taking and managing risk. They still don't need much help, though they do expect some guarantee that things won't break randomly. This is the bulk of your community.
- When you are in version two or three, you will start to attract the mass market. These are people who expect stability and reliability. They'll ask questions like, "Do you offer support?" Some of these will become contributors. Mostly, however, they are the target paying customers.
- Finally, when you are in later versions, the laggards and skeptics will finally pick up older versions and try them.

It's more complex than this, as you can have multiple overlapping curves. You need to keep the whole market interested, or you lose valuable sections of your community. Each section sells to the next, so you should aim new versions at the evangelists so they can sell them to the pioneers, and so on.

Once you understand the market curve, you see why it's counterproductive to, for instance, write perfect tutorials for the early versions. You won't get the mass market regardless and it will feel patronizing to the pioneers.

Volunteer Burnout

I've emphasized the value of volunteer work as being more accurate, honest, and creative than paid work. There's a strong caveat here. Some of the Social Architecture tools can be dangerous. When you

define a compelling mission, you can motivate people close to self-destruction. This was a major problem in the FFII before I took over, made worse by the highly emotional and tribal culture of the organization at that time. Many core members were in a state of deep exhaustion and burnout. It was familiar to me from my own past.

Research into burnout — which you can read on Wikipedia[43] — doesn't seem to match what I've observed in the real world. Data trumps theory, however. Here's what I've seen many times about the specific type of burnout we see in volunteer communities:

- It manifests as a deep disgust with a specific project. We push the project aside, stop answering emails, and might even leave the community. Other people observe that "he's acting strange... depressed, or tired..."
- It is project-related. That is, we burn out on specific projects and not on others. In severe cases, we become dysfunctional for a few months, then begin working again by abandoning the project and starting something else.
- It hits after a period of one to three years, depending on our character and the situation. Very stubborn, driven individuals may take longer to burn out, and when they do, it's worse.
- It is curable. This is the weirdest aspect, which I proved by taking burned-out volunteers and finding money to pay them for what they had been doing for free. They came back happily and carried on successfully.
- It is preventable. Paid staff don't suffer the same kind of burnout. They can definitely get depressed, yet they don't usually just switch off.

Which leads me to conclude that this is about the economics of professional investment. Here's my hypothesis of the mechanisms at play.

---

43 https://en.wikipedia.org/wiki/Occupational_burnout

Many people invest heavily in their professions, taking great risks especially while young in the hope of reaping rewards later in life. We're able to postpone material rewards for a long time if we think we're on the right track. For example, a young writer or musician will tolerate being poor for many years if he thinks he's on the path to eventual fame and fortune.

No matter how subtle, the carrot at the end of the stick is always present in our subconscious. We are essentially economic animals. All of life is economic. We can lie to ourselves really well, yet beneath every act and decision is an economic motive. We invest in projects because we feel they will propel us to success, even if it takes years. We compete with others, trying to find niches where our particular talents can shine.

So it happens that the young mind striving to invest in the right places finds itself in a situation where the weight of lies accumulates and reaches a tipping point. The path suddenly proves itself to be a dead end. The people it was following are manipulative liars. The mission was a fraud. The praise of others is emotional blackmail. The years of investment were a waste, and even a further minute would be wasted.

This type of burnout is like a reckoning. We abandon the project as though it were suddenly toxic, with much the same feeling as if we had eaten something spoiled. Here are some ways to reduce the risk of this happening:

- We cannot work alone on projects. The concentration of all of the responsibility on one person who does not set limits often leads to burnout.
- Projects need a business plan. As long as there is an eventual prospect of economic reward, the mind can survive hard work without material reward for some time.
- Preventative education on burnout can help. When we explain to people what burnout is, they recognize it faster and call for help before it is too late.

- Good tools and processes let us work with less stress and with less dependence on any one person.

The Myth of Individual Intelligence

You will have gathered by now that I'm not a great fan of the brilliance of individuals. Mostly this is because despite being a Mensa member, I've seen myself make such amazingly clever mistakes. Over time I've come to think that the very notion of individual intelligence is a dangerously simplified myth.

In this myth, brilliant individuals think about important problems, and then by hard work and labor, they create solutions and refine those until they are perfect. Sometimes they will have "eureka" moments where they "get" brilliantly simple answers to large problems. The inventor, and the process of invention are rare, precious, and can command a monopoly. History is full of such heroic individuals. We owe them our modern world.

Look more closely, however, and one discovers that this story does not match the facts. History doesn't show lone inventors. It shows lucky people who steal or claim ownership of ideas that are being worked on by many. It shows brilliant people striking lucky, and then spending decades on fruitless and pointless quests. The best-known large-scale inventors like Thomas Edison were good at systematic broad research done by large teams. It's like claiming that Steve Jobs invented every tool made by Apple. It is a nice myth, good for marketing, and utterly untrue.

Recent history, better recorded and less easy to manipulate, shows this well. The Internet is surely one of the most innovative and fast-moving areas of technology, and one of the best documented. It has no inventor. Instead, it has a massive economy of people who have carefully and progressively solved a long series of immediate problems, documented their answers, and made those available to all.

The innovative nature of the Internet comes not from a small, select band of Einsteins. It comes from RFCs anyone can use and improve,

made by hundreds and thousands of smart, though not uniquely smart, individuals. It comes from open source software that anyone can use and improve. It comes from sharing, remixing, and scale of community. It comes from the continuous accretion of good solutions, and the disposal of bad ones.

Here thus is an alternative theory of innovation:

1. There is an infinite problem/solution terrain. It is like a landscape of hills and valleys that we are trying to climb. The solutions to interesting problems are at the tops of the hills.
2. This terrain changes over time according to external conditions. Mountains can become flat, and new mountains appear, over time.
3. We can only accurately perceive problems to which we are close. We do not have very long-range vision, only guesses. Our metaphorical landscape is very misty.
4. We can rank the cost/benefit economics of problems using a market for solutions. That is, we can measure how high we are on any given peak.
5. There is an optimal solution to any solvable problem. That is, every slope has a top.
6. We can approach this optimal solution mechanically, by applying the method of taking a step in some approximately good direction, and seeing whether we are now higher or lower than before.
7. Our intelligence can make this process faster, yet does not replace it. Being smarter maybe lets us step faster, or see a little further into the mist, and that's it.

There are a few corollaries to this:

- *Individual creativity matters less than process.* Smarter people may work faster, and they may also work in the wrong direction. It's the collective vision of reality that keeps us honest and relevant.

- *We don't need road maps if we have a good process.* Functionality will emerge and evolve over time as solutions compete for market shares.
- *We don't invent solutions so much as discover them.* All sympathies to the creative soul: it is just an information processing machine that likes to polish its own ego and collect karma.
- *Intelligence is a social effect, though it feels personal.* A person cut off from others eventually stops thinking. We can neither collect problems nor measure solutions without other people.
- *The size and diversity of the community is a key factor.* Larger, more diverse communities collect more relevant problems, solve them more accurately, and do this faster than a small expert group.

So when we trust the solitary experts, they make classic mistakes. They focus on ideas, not problems. They focus on the wrong problems. They make misjudgments about the value of solving problems. And they don't use their own work.

The Collective Intelligence Index, or CII

I'm going to propose a tool to measure the intelligence of a community, in other words, how accurately and efficiently the community is working at any given time. It also measures how enjoyable it will be to participate in the community.

To demonstrate, I'm going to rank a few networks, organizations, websites, and on-line communities. It's not science; it's more like creative abuse of numbers. As everyone knows, 87% of statistics are invented on the spot and 91% of people accept them without question. I've chosen the following victims:

- Wikipedia
- Twitter
- Reddit
- Facebook
- The fashion industry

- The Nigerian movie industry, aka Nollywood
- The military (in some random western nation)
- The Fox News network
- Lawyers, as a profession
- The Hollywood movie industry

I'm not going to make any judgment about the value of any specific community. It's impossible, and would be deceptive. Twitter's implied mission is "collect the most followers," which sounds weak when compared to Wikipedia's "assemble the world's knowledge." Once formed, a smart and agile crowd can just as easily create new missions like "bring down the dictator." Arguably, the value (to society) of an on-line community is not their products, rather it is the community itself. With Wikipedia or ZeroMQ, it's hard to separate the crowd from the content. With Twitter, it's really obvious. The content is transient and mostly worthless, the crowd is not.

Here's the scorecard I came up with:

Criteria	*Wk*	*Tw*	*Rd*	*Fb*	*Fa*	*Nw*	*Lw*	*Hw*	*FN*	*Ml*
Strong mission	5	3	2	1	2	1	0	0	0	2
Free entry	5	5	5	5	4	3	0	1	2	2
Transparency	5	3	5	1	2	1	0	0	0	0
Free contributors	5	5	5	5	2	3	3	2	1	0
Full remixability	5	5	5	4	4	3	3	1	1	0
Strong protocols	5	5	5	4	4	3	2	3	1	4
Fair authority	5	4	5	3	4	3	1	1	0	1
Non-tribalism	4	5	5	5	3	3	0	2	0	0
Self-organization	5	5	5	5	4	4	2	2	0	0
Tolerance	5	5	5	5	4	3	2	3	0	0
Measurable success	5	5	5	5	5	5	4	5	5	2
High scoring	3	5	5	5	4	3	3	2	1	1
Decentralization	5	5	5	5	5	1	1	1	0	1
Free workspaces	5	5	5	5	3	2	0	0	0	0
Smooth learning	4	5	5	5	3	3	0	1	0	0
Regular structure	5	5	5	4	3	2	3	3	1	5

Positivity	5	5	5	5	5	3	0	2	0	0
Sense of humor	5	5	5	5	2	3	0	1	1	0
Minimalism	5	5	4	4	3	4	1	1	3	0
Sane funding	5	4	3	3	5	3	3	3	2	2
Final score	*96*	*94*	*94*	*84*	*71*	*56*	*28*	*34*	*18*	*20*

Once we can measure the CII of a community or organization, we can increase it by looking at the tools that score low. In theory, this should make the organization smarter, and its participants happier. Of course it's quite likely that a military organization can only work with a low CII. A smart army would quite likely all go home and switch to Reddit.

Final Thoughts

This chapter was a handbook for building on-line communities out of little more than insane ambition, using the pop science of Social Architecture. If there's one thing we learned, it's that *how we organize* matters much more than *who we are*.

We looked at 20 tools that I've learned are helpful in designing and growing large, healthy wise crowds. These tools came from years of work in politics and free software development.

The overall message of this chapter was essentially humanistic and optimistic. It holds that people are generally good, and will naturally work together to do great things and fix the world. In the next chapter, we'll dig into the dark side of crowds in order to understand why good people can do terrible things when put in the wrong situations.

Chapter 3. Faceless Societies

> *The Empire was run by an old, faceless society of criminals. It ran on cheap oil and cheap blood. It smashed its opponents in the name of Peace.*

Just as good on any scale can emanate from a wise crowd, large amounts of bad can arise from a mad mob. It's not about individuals. Rather, it's about how groups organize and are organized. In this chapter we ask, "*If humans are programmed to do good, how does one explain our amazing talent for doing bad?*" We will examine recipes for turning a wise crowd into a mad mob, and perhaps find paths to fix some large-scale mad mobs in future.

Humanity as a Wise Crowd

We live in a physical universe, and *everything* in it obeys physical laws that operate on many levels, from the quantum to the galactic. Each level has its own truths, all approximate, yet accurate enough to work. The progress of human culture has been to understand more and more of these truths. As we understand more, we move problems from the domain of belief (where the answers are long, complex, and superficial) into the domain of evidence-based knowledge (where the answers tend to be shorter, simpler, and more profound). At no stage has anyone done the reverse — to prove that evidence-based science *is not* the best way to solve problems. Nor has this process slowed down; indeed, it moves faster each day.

Human culture seems to have evolved to mine truths. Like the ancient bacterial colonies that filtered particles of gold from the sea and laid them down over millions of years to form gold deposits, human society acts as an information-processing machine. Each individual mind, for purely selfish reasons, collaborates with others to turn observed data into patterns of information, and then into reusable tools,

in other words, knowledge. "Information" is shorthand for "data, information, and knowledge."

Collective intelligence operates as a social network that collects interesting problems. It then solves these by casting around for as many solutions as possible — even insane ones. It filters and remixes these solutions, testing them against known facts. It tries them out in as many diverse situations as possible. It finally reduces the set of possible answers down to minimal packages that can be traded and carried across generations. The better the collective intelligence, the faster it works and the more accurate and useful its results. The more these results approach general truths, the more useful they are, to more people.

Collective intelligence needs ways to shift information around. Importantly, it must assign the right value to everything because otherwise it cannot filter out the rare and valuably accurate pieces of information from the vast majority of junk. The best mechanism appears to be that each peer in the network places a value on the information they share or are offered and work accordingly. It's not as simple as placing a monetary cost on a whispered secret.

Rather, peers value other peers for their ability to deliver useful information over time, and peers will maintain notions of information credit and debt with respect to others. We can try to model collective intelligences as economies of information that operate according to the principles of specialization and trade in a free market.

The basic rules for moving information around human society are economics. We specialize in our favored areas, and we trade information about those areas in what is ideally a free market. The ability to properly value and trade information with other people is a sign of adulthood. A teenager is mature when he or she can take part "in adult conversation," which essentially means entering the information market.

And so the jet I am flying in is more "accurate" than the planes of a century ago. It is faster, carries more people, is safer, travels further,

and consumes less fuel per passenger mile. It is *a truth*: the result of vast numbers of information exchanges between individuals and groups.

Looking at successful on-line communities from a distance, we see human society in its most general form. Our history, over millions of years, is a long story of meeting stark challenges with radical cultural and technological innovation. Obviously, our species is the descendants of tough and smart survivors who found an answer for every single problem facing the family for over 3.5 billion years, the dawn of life. High five! For all its many inefficiencies and dark aspects, post-ape human culture has been remarkably adaptable and successful. It seems fair to assume that the earliest roots of our particularly human culture grew from our ability to think collectively as well as reason individually.

How can I make such a broad statement? Well, it seems clear that the mental tools we need in order to construct wise crowds are built into our minds; they have evolved and were not learned. I'm not just thinking of the language instinct, though this is clearly fundamental. I'm also thinking of what I consider the social instincts, such as respect for authority and rules, willingness to collaborate, intolerance of cheaters, strength of identity, pride of accomplishment, memory of others' accomplishments, ability to calculate collective rankings, and so on. These are instinctive — visible in young children without prompting, consistent across all human societies, and irrepressible no matter what pressure is applied.

Yet one nagging question comes back: Why is there so much stupidity in the world when we're apparently so well equipped to act as wise crowds? The answer is that sometimes stupidity beats wisdom, and just as we're born with the talent to create, we're born with the ability to destroy. Wise crowds have the potential to become mad mobs, as you'll see in the following scenarios.

Sports Break

I remember the warm, late Brussels summer of 2000. Belgium was hosting the "Euro 2000" football tournament. Every day for several weeks, a match was played between two national teams, and every evening, two tribes of opposing fans would fill the Brussels city center — the winning team parading for hours in open cars, honking and cheering, the losing team scowling in the shadows and drinking, and thousands of participants joining the raucous unplanned street parties.

After about two weeks of increasingly noisy nights, which began to turn to violence, the police moved in with riot gear. Surprised and confused tourists taking the wrong turn through the historic heart of Brussels found themselves trapped between crowds of noisy beer-sodden youths throwing cans and dropping their trousers, and baton-waving riot police.

As the police resorted to dogs and tear gas, the rioters began pulling up Brussels' famous cobblestones and using them to demolish restaurants and bars in the old center. I watched as the shocked patrons, lips still wet from after-dinner cognac, upturned tables to use as shields against incoming rocks. Then groups of plain-clothed policemen arrived and grabbed the rioters, using plastic cable ties to stop them from running away.

The riots turned from simple national vanity to full-on battles between Brussels' disaffected unemployed youth and the State. Groups of masked youths ran up and down Brussels' alleyways looking for fights, while TV camera crews looking for footage tried to keep up. Heavily protected policewomen, followed later by much tougher policemen with shields and batons and dogs, tried to keep control. The police blocked off entire sections of the city center, squads of them chasing off or arresting the rioters. Despite that, the scene got more and more ugly, and violent running battles started to erupt.

Then someone had the elegantly simple idea of turning off all the street lamps in the city center. Suddenly, there was dark, and almost instant peace. The youths could not see where to go. The TV cameramen could not shoot their scenes. And the police could continue cordoning off the old city, street by street, until it was swept clean of troublemakers.

The Face in the Mirror

What causes crowds — both the rioters and the police — to become so stupid? Can we even define what "stupid" means? The answer lies in the concept of *truth* and how efficiently the collective intelligence mines truth from the raw data the universe presents.

Listen to the cry of a crazy crowd speaking about a social minority or otherwise perceived alien threat: "They are parasites and we must eradicate them all!" Here's a stupid crowd: "Ooh, burning police cars! That's fun. Let's also smash some windows!" To get a grip on what can seem like utter chaos, we need to see such patterns as inherently rational ones that tipped into dysfunction for various reasons. There is method in madness. When we see the method, we are better equipped to deal with the madness.

In 2011, Anders Breivik calmly tried to start a civil war in Europe by murdering what he called "category B and C traitors" in a series of sequential shootings and bombings in Oslo, Norway. His 1,518-page manifesto is the brain dump of an intelligent, educated, highly conscious, and utterly insane individual. It is not political any more than it is religious. He compiles a world of mostly mythological or false material, taking only that which confirms his biases and insecurities, turns that into a painfully detailed rationalization and plan, and then uses that to commit acts of pure horror.

Breivik's internal fractures turn into catastrophic mental failure as he reaches adulthood. Instead of getting help, he finds his life's cause in the politics of hate that are sweeping Europe, in cult-like far-right groups, and in shadowy paramilitary networks. Immigration often

provokes resentment, and politicians can play on that. We hope that everyone understands it's a game. Most do, except minds like Breivik, who use the "Islamic threat" as a mental life jacket. The more he can blame Marxists, feminists, and Muslims, the more he can frame his mental fracture as enlightenment, and his isolationist and psychopathic tendencies as a warrior spirit.

So while politicians play with fire, Breivik's very mental survival depends on his burning down the house. The more time and money he invests in his delusion, the more it becomes his reality. And then his reality collides with ours, children die, and he sits calmly in prison waiting for his time at the microphone.

Because collective psychology is an expression of individual psychology, and this book is essentially about how we are working together to build a new world, let's put on the psychologist's hat and examine mental disorders. If we can understand how individual mental disorders can be "rational," perhaps we can apply the same approach to collective madness.

Mental disorders range from caffeine addiction (yes, seriously, it is in the book) to murderous psychopathy. I'll look specifically at personality disorders, which compose half of psychiatric cases, and cover how we as individuals malfunction in society. As Wikipedia notes[44], "a person is classified as having a personality disorder if their abnormalities of behavior impair their social or occupational functioning."

The Borgia Hypothesis

The *Diagnostic and Statistical Manual of Mental Disorders*[45], aka DSM, is the bible of Psychiatry, and lists about 300 mental disorders. The disorders are categorized in various dimensions. DSM makes interesting reading[46]. What's particularly striking is how many symp-

44 https://en.wikipedia.org/wiki/Personality_disorder

45 https://en.wikipedia.org/wiki/Diagnostic_and_Statistical_Manual_of_Mental_Disorders

46 http://www.psychiatryonline.com/DSMPDF/dsm-iv.pdf

toms of personality disorders are present in general society, people we know, and even ourselves if we look carefully.

For example, in business executives[47], histrionic personality disorder, narcissistic personality disorder, and obsessive-compulsive personality disorder scores were as high or higher than that of disturbed criminals.

A widely-held explanation for personality disorders is poor parenting and/or abuse. If your daughter has borderline personality disorder, the assumption is often that she had bad or abusive parents. It seems a double punishment for those with troubled children. It also raises disturbing questions about how to intervene if, for instance, tests show a young child starting to show symptoms of a personality disorder. Do we remove them from their (failing, according to mental health professionals) family and put them into foster care? Or do we leave them in place, and administer drugs?

The upbringing/abuse explanation concludes that people are fragile, easily broken, and only lifelong support from drugs and therapy can help them. It has two outcomes: to increase the number of people taking expensive drugs and therapy, and to fracture the families of those who are most vulnerable.

The alternative explanation, backed by a growing body of data, is biological basis. It is still a controversial notion, absent from DSM-5, which was authored by the pharmaceutical and mental health care industries. A biological basis means that personality disorders are strongly inherited, and triggered or exacerbated by environmental factors to a degree that we can actually measure, from twin studies.

Yet within this exists a paradox: How can genes that make us so dysfunctional, self-destructive, and even suicidal be the result of natural selection? The same paradox applies to groups: How can collective violence and stupidity be based on inheritable instincts when they clearly seem counterproductive?

---

47 https://en.wikipedia.org/wiki/Personality_disorder#In_executives

The simplest plausible answer is that "being functional" is *highly context-sensitive*. In societies with enough food, being tall is advantageous. In societies that live on ecological margins, being short is an advantage. The results: tall cattle herders and short forest pygmies. Your genes define how tall you might become, and your health and diet — and that of your mother — defines how tall you actually do become. In a tribe of herders, the shortest men won't have children unless they're particularly smart or funny. And in a tribe of pygmies, there will be a tall lanky woman who keeps hitting her head against the branches.

Personality disorders — like autism — all have a spectrum of symptoms from mild and widely distributed, to severe and rare. A Norwegian study[48] found a general incidence of 13% (one in eight of the population) for any personality disorder, with rates for individual disorders ranging from 1% or less (borderline personality disorder) to 5% (avoidant personality disorder).

When we classify, say, severe psychopaths as sick people, are we missing the clue that this way of interacting with the world can be highly successful? Even in our modern world, sometimes the only difference between dangerous criminals and highly paid executives seems to be getting caught. In some societies, like southern Italy, US Congress, or Wall Street, criminals and successful businessmen are interchangeable.

And subconsciously, we seem to value personality disorders as long as they don't touch us personally. The heroes and heroines of popular culture are often extraordinarily violent, manipulative, or emotional. A small amount of instability makes people attractive to others as long as it's combined with intelligence and beauty. Many men classify women along a "crazy-beautiful" scale. It's not just that we men tolerate more craziness in prettier women; we expect it. And as Waylon Jennings sings, ladies love outlaws.

---

48 http://archpsyc.jamanetwork.com/article.aspx?articleid=481789

So taking the theory of a biological basis for personality disorders and adding a heavy layer of "sometimes you have to be crazy to survive," I'll propose the "Borgia Hypothesis" of personality disorders after Cesare Borgia, the model for Machiavelli's "Prince," who shocked da Vinci and Machiavelli[49] with his "amoral and pragmatic methods."

The Borgia Hypothesis says that personality disorders are evolved aspects of social behavior, and that they have a biological basis. Further, these aspects are not diseases, they are indeed powerful assets in certain situations. However, they can become dysfunctional in societies that have no use for them. In a violent and unstable society, being manipulative, charming, egocentric, and lacking all empathy for others is a winning strategy. In a peaceful and stable society, it is a dangerous mental disorder. In some circumstances, the ability to instantly project powerful emotions is a key to survival. In others, it is disruptive and antisocial.

Any inherited talent needs culture to grow in. Our innate talents will often shrivel and die without opportunity to learn from others, and practice. Genes need culture, and culture needs genes. To argue between genes and upbringing is to entirely miss the point. Further, genes will express themselves in different ways and degrees, over time and according to circumstances. Gene expression is an incredibly complex aspect of biology that we're just beginning to understand.

Genes can stay inactive for decades, then switch on, triggered by a cascade of other genes suddenly doing something a little differently. And it's specific to every type of cell in our bodies. This, together with the evidence that there are many genes involved explains the "spectrum." A person may have more of fewer of the responsible genes, copies from one parent, or both, and the genes may switch on and off during their lifetime depending on factors such as being in abusive situations.

---

49 http://articles.washingtonpost.com/2010-01-31/news/36899052_1_cesare-borgia-renaissance-man-savvy-diplomat

The hypothesis is therefore that the genetic infrastructure for personality disorders is present in different degrees in most people, and is there because it has real survival benefits and bearable costs. It's like sickle-cell disease, which protects most carriers (one in four in equatorial Africa) from the deadly malaria parasite at a fatal cost to the one in four of carriers who get two copies. If these genes were really uneconomic (if their costs outweighed their benefits), they would gradually disappear, like the genes for tails or full body hair.

This hypothesis is much more optimistic than the "people get broken or sick" argument. It means we can recognize vulnerable babies and children simply by tracking parents who have difficulties. We don't need to wait until they show symptoms. It means we can search for the plausible social triggers and address them. It may simply be that while all children need socialization, those who carry severe personality disorders just need more love, physical play, and emotional security than most. Presumably, as for language, we have critical learning periods when young, and we can still learn on top of that, all our life long.

Can adult sufferers be cured rather than treated with drugs and therapy? I'm not going to speculate on whether these genes can switch off or explore what kind of environments might be able to do this. I do have a question for the mental health profession. If personality disorders are (for the sake of argument) a programmed response to certain social triggers, are drugs and therapy really going to change the sufferer's interaction with society?

Natural Born Killers

In the twentieth century, there were two main schools of thought regarding humanity's bad habits. The first was that these were cultural and could be fixed by imposing cultural change. The second was that they were genetic and could be fixed by steering natural selection. Both views led to massive violence and suffering, proving first that it requires great force to bend society in any direction and second, that

trying to fix society by force is itself an insane act. G. K. Chesterton, an early critic of eugenics, wrote of the United Kingdom's Eugenics Laws that "the State has suddenly and quietly gone mad. It is talking nonsense and it can't stop."

If there was consensus by the late twentieth century, it was that trying to change society by selectively killing or sterilizing those we considered "unfit" was worse than mass brainwashing. We would tolerate dictators as long as there wasn't mass murder going on. Actually I think selective breeding of humans has a worse name to it than mass murder.

However, around the end of the twentieth century, evolutionary psychologists began to uncover some rather different truths about human nature. The first was that it most definitely evolved. The second was that the evolution was carried both in genes and in culture, inseparably. Without learning, our inborn mental tools can't develop. All human languages come from a single common ancestor, just as all human genes do. Third, human nature, like culture, is a rich collection of strategies, which we can select and shape according to need. Our ability to adapt our mental toolset to new circumstance is as much a product of our evolution as the toolset itself.

Thus, instincts are our basic inherited toolset, and culture is the learned strategic expression of those tools. We are born with instincts for sharing, fairness, and collaboration. We are also born with instincts for opportunism, deception, and violence. Depending on the economics of the culture in which we grow up — which may depend on geography — we select, develop, and sharpen certain instincts over others.

To appreciate human culture, you have to be able to abstract yourself from it. This is a bit like appreciating the beauty of all life even as one tries to kill a mosquito. All culture, no matter how strange, is born from a survival strategy. There is no "forwards" and no "backwards," except from the seat of our own prejudices. We can and should strive for fairer, more pleasant societies, yet there is no basis for

claiming that these are *better* in any objective sense. Having said this, from my own highly prejudiced seat, it's *definitely* better to live in a freer and less violent society, and this is the viewpoint I take in this book.

The science that sociologists should practice is this: observe people in their best and worst moments. Then, reverse-engineer the underlying instincts that are at work, if necessary by analogy with other animals. This is what evolutionary psychologists do. Then, the sociologists should create hypotheses about which cultural strategies are at work, try to disprove these hypotheses, and eventually use the surviving hypotheses as guides for social regulation.

Let's go back to violence. The majority of male-on-male violence is and always has been either over access to or control over women, or over status. These are much the same thing in the politically incorrect male mind. Honor feuds are a fact of life for most pre-industrial societies, and they typically run between families to the extent that new tribes are often the product of a feud that forces one individual to leave, together with his close family[50].

It makes sense to assume that instincts for attachment to and violent defense of the tribe and tribal territory are deeply embedded in the human psyche and genome. The human story has often played out in pockets of valuable territory — refuges of fertility, security, food and water — embedded in wastelands of semi-desert or forest. Until about 500 years ago, most of humanity lived where their ancestors first settled, having pushed out any previous owners. The main migrations as we walked away from or through Africa were either into empty territory made accessible by lower sea levels and retreating ice caps, or away from encroaching deserts and ice caps.

Over millions of years, groups of our ancestors repeatedly clashed over water, food, and above all, territory. Any group that split and ran would be exterminated. Individual preservation means nothing. Survival when attacked lies in loyalty to the group, following others, and

50 https://en.wikipedia.org/wiki/Erik_the_Red

the ability to react violently and emotionally to defend the tribal turf. He who runs away may live to fight another day, yet we are like gazelles. Lone survivors tend to be picked off quickly. We don't generally scatter and flee when confronted; we gather together, and we fight.

This is deeply embedded in our ethos and mythos. The hero is not the one who escapes; he's the one who prevails. This is worth repeating because if cowardice were a successful strategy, it'd be sexy. The market is brutal about how it values genes with survival value. The hero in the zombie movie either stays and fights, or runs to save his family.

Of course in most times and locations, life is not confrontational. Though we notice the wars, they are spaced with long periods of peace, and Steven Pinker has argued convincingly that over time society has become progressively more peaceful[51]. The thing about violent confrontation is that it takes just one mistake to lose one's life. Peace is not risky, yet being too nice in a time of violence is the kind of mistake that wipes out entire genetic lines. I'd expect our genetic heritage to keep a knife-edge balance between too much and too little capacity for aggressive tribalism.

History shows that most of us carry the instinct for murder — or at least for physically violent self-defense — and also strong instincts for suppressing violence. Most conflicts are not violent; they are just jostling for relative advantage. We've sublimated huge chunks of our tribal violence into sports, politics, and other non-lethal status competitions. Males do this in many species. Male elephants and walruses fight over dominance, nonetheless, those tusks are mainly for show and intimidation, not murder. In addition to a potential threat, other people represent a valuable genetic and economic resource. Only a broken society driven by insane leadership actually moves to mass killings.

---

51 http://stevenpinker.com/publications/better-angels-our-nature

As human society has gotten more sophisticated and less dependent on raw natural resources, it has also devalued the need for strong tribal emotions, particularly male aggression. We can achieve much more today by dialogue and trade than by simple force. Still, our instincts for tribalism are deep and old, and only superficially controlled. They come out easily when provoked. Ask someone where "they are from," then say something less than polite about that country, and watch the reaction.

One can draw two male caricatures: the "jocks" and the "nerds." The jocks tend to sports; the nerds to intellectual pursuits. Speaking as an intellectual, I can vouch shamelessly that nerds are more intelligent, have better looks and genes, and are more likely to thrive in digital society. However, I've never met a male — jock or nerd — that was immune to tribalism. The main difference is that the jocks do it without comment, as if it were obvious.

The nerds, on the other hand, back their tribalism with endless self-justification that can turn into formalized dogmatic collective insanity in the worst cases. The jocks may be the ones shouting and wielding the sticks. However, it's the nerds who invent the slogans and ideologies and build the political machines behind the genocides.

Stupid, Mad, or Bad

A Serbian soldier in Bosnia, when asked by a journalist why they had not opposed NATO, after so many years of swearing they would die to build a Greater Serbia said, "We may be mad. We're not stupid." I speak sometimes of madness, sometimes of stupidity. When we speak of an individual, the two properties are quite different, as the Serbian soldier tried to explain. When we speak of a large group of people, madness and stupidity look almost the same.

In general, collective stupidity is a precursor to collective madness. When someone asks me to explain Nazi Germany — this happens almost daily on the street, I swear — I give this explanation:

"*By 1930, Germans were collectively stupid, having suffered a war, the loss of empire, punitive reparations, and hyperinflation. The German middle classes, especially, were bankrupted and in a state of shock. This made them easy prey for an aggressive takeover by a small group of malign psychopaths who rightly saw the weakened German state and depressed middle classes as vulnerable.*

"*Using nationalism, xenophobia, and racism, these thugs took control over the state via the ballot box. They then built a cult-like power system increasingly based on propaganda, a climate of fear, and selective brutality. In 1933 they were strong enough to stage a coup and create a one-party state. The Nazi party took control of the army, and from 1934 to 1939 instituted a dictatorship based on fear and elimination of all dissent.*

"*By 1939, Germany had gone collectively insane to the point where it committed genocide and then self-destructed in an all-fronts war it could never win.*"

I realize that there are many more complex explanations. Mostly they try to blame the German people in some general way, or else they focus on the relationships between the Jewish community and its host nation. My answer to such explanations is: by treating this as a special case, you learn nothing — or you learn the wrong lessons. Everything is a special case; you learn by finding the common patterns. The pattern here is: when a clique of thugs decides to take over a country, they have to first make it stupider and then keep it as stupid, afraid, and insecure as possible. This is priority number one for an old political elite or new junta that has something less than peace and reconstruction in mind.

Sporting Colors

History tells[52] stories of entire cities driven by rivalries over symbols and colors. Set a class of teenagers in a hall, divide them into two, give one half blue arm bands and the other red arm bands, say nothing more, and watch what happens. They will mill around, abandoning friends with the "wrong" color and sticking closer to those with the same color. The two sides will measure each other and see which is superior. If there is a clear difference, the weaker group will cow and lower their heads. If they are equally matched, the two groups will move silently towards confrontation.

There are variations on this experiment. Ask just half a class to wear arm bands of one color for a week. At the end of the week, ask who found the experience enjoyable — those with the arm bands or those without. Now repeat the same experiment with another class, and this time get the teacher to also wear the arm band for the week. This happened in Constantinople during the time of the Nika riots, when the Emperor chose the blue side. The result was near civil war between the loyal blues and the rebel reds.

These are easy exercises that demonstrate how random and petty it is to divide groups. I haven't actually tried the first experiment, however, apparently in American summer camps, they do this regularly, calling it "color wars"[53]. My sister Dr. Helen Hintjens demonstrates the emotional impact of unfair land distribution before the Rwandan genocide by giving some of her class several chocolates, some none, and then taking a five-minute break. After, she'd ask them to express how they felt. Those without chocolates would feel angry and jealous.

However, while some ate their chocolates, and felt guilty and fearful, some would share their chocolates, and others would come back to the teacher with the chocolates uneaten, to ask what on earth she

52 https://en.wikipedia.org/wiki/Nika_riots

53 http://www.thisamericanlife.org/radio-archives/episode/109/notes-on-camp

was playing at. As Dr Hintjens says, "Which all went to prove the point that there are more than two (greed or grievance) possible responses to every situation of blatant injustice."

Economic inequality can create strong negative emotions on both sides. This isn't the only way to divide people and create a mad mob. Here are some other techniques:

- Anything related to sports or politics, as in the US, where politics is a form of sport. I've argued that our violent heritage is sublimated into sports. That makes sports an easy trigger for divisive antagonism.
- Any situation where there are spectators to witness and enjoy a conflict, from the Roman amphitheaters to the Iraq wars.
- Focus on issues that invoke tribalism: ethnicity, language, religion, race, and even class.
- Focus on issues that create strong negative emotions: immigration, gay marriage, gun ownership, religion, race.

Although I don't aim to be a political writer, politics does often provide the most tangible examples of mad mobs. US politics has all of the above criteria and has produced nonsensical results like the election of transparently incompetent and unethical presidents. A cynical observer would see deliberate strategy at work here. Drive public opinion towards stupidity by focusing debate on unsolvable emotional or tribalistic issues. Create spectator masses through television. Give political events the same look and feel as sporting events, including cheerleaders dressed up as Fox News anchors. I'd argue that mainstream US political parties are like the Nika red and blue arm bands: symbols of division lacking any substance.

If we accept this analysis that US politics is largely about *not* discussing the real issues, it should be a simple (though in practice, nearly impossible) recipe to turn the mad mob of US democracy into a boring yet sane wise crowd. First, ban television coverage of party politics and televised political advertisements, no matter who pays. Second, treat discussions of religion, race, ethnicity, or language in political de-

bates as immoral, rude, and unethical. Third, ban public political events. Last, ban party colors, slogans, and other tribal marketing.

You might say such a democracy could never function. Nonetheless, there are actually quite a few countries where this is more or less how things work. They tend to produce boring yet competent governments that do not steal billions, do not declare war on other countries, and do not spy on their own citizens. Much of Europe is governed by such policies, formal or informal. The only cases in Europe where government starts to go mad is where tribalism gets added to the mix, like Belgium in certain seasons. From June 2010 to December 2011, Belgium had no federal government at all, and worked well enough for those of us living here at the time.

Stupidity is Not Random

I've looked at some main causes for mad mobs: territory, tribalism, religion, sports, and politics. There are many factors that make groups less intelligent without turning them into hooligans. There are degrees and shades. Here are some things that I think make people collectively stupider. They're not all that obvious:

- *Television*. TV must be one of the most costly inventions ever in terms of direct productivity wasted through lost time, and indirectly through lower overall intelligence of a TV-viewing public. Why does watching TV make us stupider? It has a very strong effect on how we see the world. When millions of people see the same programs, their overall diversity of opinion seems to fall dramatically. This effect is obvious with propaganda TV, however it's present in all mass media.
- *Team sports*. Beach volleyball, granted, can make good viewing. Team sports, however, express the essence of tribalism, sometimes violently. You don't hear of chess riots or origami hooligans. Many mass activities, like pop festivals, even with the addition of lots of

drugs and alcohol, do not end in running street fights. Team sports often do end in chaos[54].

- *Belief in the supernatural*. Religion has its uses, like all our social instincts (this is my story, take it or leave it). It lets us delegate responsibility for disasters that have no logical explanation, so we can keep our logic safe for things we do understand. Without the fusebox of belief in an imaginary supernatural, we'd have to analyze and solve every single flood, drought, illness, accident, and social injustice. And since the world is full of disasters beyond our control, we'd go crazy.

Normally, as science explains more of the world around us and technology makes our world more predictable, religion should decrease. This seems to be the way it works. Religion definitely makes individuals more dull witted, and groups stupid. Organized religion scores very low on the Collective Intelligence Index.

- *Tribalism*. All modern humans descended from about 10,000 individuals who lived about 300,000 years ago, and all non-African humans from a far smaller selection. Anyone who thinks their particular family tree makes them special is as crazy as a Cardinal. True, some genes seem more fit than others, and some family trees have more of these genes. However, there is zero correspondence between good genes and "ethnic origin," except in reverse: the more isolated and homogeneous a gene pool is, the more likely it is to be filled with bugs.

The evolutionary justification for tribalism ended perhaps 5,000 years ago when the technologies of agriculture, portable trade goods, and currencies made it more profitable to work collectively than to fight over patches of hunting ground, watering holes, or trade routes.

- *Language identity*. Digital society specializes in intense and useless fights called "language wars." When we get attached to languages, that makes us dim witted. All languages are good for something.

54 https://www.google.com/search?q=hockey+football+riots

> French for arguments: you can shout for ten minutes and say nothing. English for business: it's easy to pick up yet hard to master. German for poetry... well, just because. Japanese for secrets: it is really four languages depending on who you're talking to. Italian for traffic directions: it involves much hand-waving. Spanish for stories, because of the wine.

A language is like a social credit card, and a pragmatic person learns as many languages as he or she can afford. One should never *belong* to a language.

- *Anything that homogenizes our lives.* This is a long list, because industrial society is so good at producing endless identical products: same cars, houses, clothes, food, music, gadgets, and culture. There is a direct causal relationship between the cookie-cutter sprawl of US life, and the inability of most of American society to develop sophisticated answers to elemental questions such as "How free should a person be?" Europe is sometimes mocked for having too many languages and too many borders, yet it is Europe's diversity that has kept this continent more or less sane since the end of WWII and European empires.

Society Versus the Individual

In my last year at school, I realized that many works of literature could be cast as a struggle between the individual and society. Lord of the Flies, 1984, Death of a Salesman, A Tale of Two Cities, you name it. It's a classic theme, central to the very concept of existence, and retold countless times. I aced my English Literature exam. However, the story is mostly only half-told. George Orwell's real message is that tyranny must crush the individual spirit to survive. In other words, if a political elite wants to prevent the rise of a wise society that would overthrow it and replace it with a meritocracy, it should attack the individuals' ability to form wise crowds in the first place.

The state of US political debate may be the accidental result of a young culture that has not developed enough authentic depth and in-

teresting cities. Or, it may be that the eradication of free thought and the creation of mad mobs are long-standing goals of those in power. Why, you might ask, do ruling classes work so hard to keep society weak? Surely happiness and prosperity are good for all? The answer is one we saw in the story of Africa. Not only do ruling elites often try to use the law and politics to work in their own interests as long as possible, they try to escape all accountability for it afterwards.

It's not just corrupt political elites that abuse their citizens. Big business, armies, prisons, boarding schools, religions, indeed many of the institutions of industrial society operate by squeezing part or all of the individuality out of people. In the worst cases, people become utterly compliant, willing to do anything, including killing themselves and others, for what they perceive as the good of the group. In the best cases, they just take a lot of abuse without complaining.

It's not an accusation against right-wing capitalism, though that has been an excuse for massive abuse of individual rights. The twentieth century also saw many "collective" left-wing societies that were notable for their ruthless suppression of individual rights. "Collective intelligence" does not mean that collectives are intelligent, any more than "horse power" means that horses have the right to vote.

1984 was a warning, not an instruction manual, and few people have explained how to really build a cult, religion, or totalitarian state. An excellent essay by Dr. Lee Carter[55] from 1989 is the best explanation I've read. He writes, "As I hope to demonstrate, these principles have been applied to most religious and political movements of the past, and will undoubtedly be applied to new ones in the future. By being aware of these techniques, the reader can be forewarned."

We spoke of personality disorders. It's been said that you can spot a psychopath by the little cloud of followers he or she drags around. Psychopaths can be vicious about spotting and exploiting peoples' weaknesses in order to make people useful for them. At the heart of every little cult is a malign psychopath, surrounded by people and yet

55 http://www.miltontimmons.com/MindControl.html

a loner. At the heart of every dictatorship, political movement, large business, or religion is a fraternity of malign psychopaths.

There are, of course, decent people who are "pro-social" psychopaths, and malign people who show no symptoms of psychopathy at all. To avoid having to say "malign psychopath" over and over, I'm going to give such individuals a more suitable label, which is "bandit." The bandits make it their business to exploit others, on a massive scale.

How do you manipulate people on the scale of an entire country? In the Art of War, Sun Tzu wrote, "*the control of a large force is the same principle as the control of a few men: it is merely a question of dividing up their numbers.*" In other words, a pattern that works for a few people can be scaled up to work for millions.

Just as a Social Architect can create a wise crowd by deliberate design, a bandit can build a gang, which is a specific type of mad mob. A gang can be *very* lucrative. And where there's money, there are expensive consultants. I'm pretty sure there has been a lot of secret, well-funded research both by private groups and governments into what I'm going to explain. You may even find the research conducted in broad daylight, if you look for it.

How The Bandit Got His Gang

Brian: I'm not the Messiah!

Arthur: I say you are, lord, and I should know... I've followed a few.

Let's start with the overall process. It is very similar to how we built an on-line community, except we take the tools from "Spheres of Light" and turn the dials down to absolute zero: insane rules, arbitrary authority, no freedom, and so on.

Every gang starts with a charismatic founder and some promise of salvation. The founder is a middle-aged, decent looking man, usually, who has been playing ping-pong with people since he could hold a

bat. By the time he is forty, he has collected a small cloud of dedicated followers, and more importantly, he has attracted one or two fellow bandits — less handsome, and harder-working — who smell an opportunity. These are the ones who will build the cloud up to something big.

The market curve applies to the bandit's gang just as it does for on-line communities, and indeed the two are hard to distinguish at the start. The first to join the cloud are the fanatics, who know the Messiah when they see him. Then come the pioneers, the early adopters, the mass market, the late adopters, and finally, the stragglers. Let's face it: if you're converting to Catholicism today, you are a straggler.

The first marketing wave goes out to people who are somewhat disconnected already. They have some issues. The bandits whisper stories about imaginary enemies and conspiracies and this draws in the low-hanging fruit, those with paranoia and other vulnerabilities. Then the bandits create a dichotomy between "them versus us" that targets the next slice of the market. Then they switch to the "Everyone is doing it, you should, too" argument to catch the mass market. Finally, they use "If you aren't with us, you are against us" to catch the late adopters.

It's not enough to just get new recruits. It is utterly vital to stop those who have already joined from leaving. The difference between a successful gang of bandits and a lone bandit is twofold. One, how well he controls his followers. Two, how effectively he stops them from leaving. In George Orwell's 1984, there was no escape of course. This is the nightmare of a society built inside walls, be they the walls of a boarding school (where I received my education in this topic), prison, or totalitarian state. For most of the growth period of even a nationwide gang — say, the German Nazi party from 1920 to 1930 — there is some possibility of escape, and there is some resistance.

So we come back to the individual and the insane society trying to control his or her mind, to eliminate both resistance and escape. Since

"fight or flight" is a very deep instinct, it's not a simple process. Fittingly, only bandits are immune to other bandits.

Week One: Losing Myself

"I've been to a few meetings, and these seem like nice, sincere people. They've offered me a place to sleep for a few days, which is great since I've been on the streets for weeks now. We all sleep in big rooms, the men in one room and the women in another building. When we get up each morning, we make our beds and sweep the floor. Like everyone, I have a small locker for my stuff. The guy next to me told me to throw away anything I didn't really need. They give you everything here, he said. I told him I wasn't staying long so it was OK.

"Breakfast was white bread, a slice of cheese, and tea without sugar. Since it's a special day (I didn't remember what exactly), we all got a fried egg too. My friend did not come to breakfast. When I saw him later, he looked hungry and pale and didn't speak to me about it.

"Then, task assignment. This is how we pay for our board and lodgings. Work is good for you, the stern matron said as she pinned up a sheet with names and assignments. I wasn't on the list. "You are still a guest," she told me without a smile when I asked about it.

"During the day I wanted to get a book from the dorm. The door was locked. Not allowed, they told me. Because I had nothing to do, I spent the day in the common room. No TV, no Internet, and no people to talk to. Everyone was busy. I read some books, which were all the same kind of stuff — stories about the organization and its founder, someone called Father, and all the good things they do. Part of my mind laughed at that, and then it was lunchtime.

"Lunch was soup, the same bread, and then mashed potatoes with sausages and cabbage. I don't know what they did to those sausages to make them both burnt and gray. I was very hungry so I ate most of it anyhow. My friend was there and ate silently. When I was done, he quickly switched trays, and ate my leftovers. When I spoke to him, other people told me to stay quiet. The matron came and scolded me,

we don't talk when we eat, she said, it's disrespectful. My face burned with shame. I guess it's their custom.

"That afternoon, we went to the main hall for recitals. Everyone had the same book with them, which I remembered from the common area library. I didn't have a book. I asked my friend and he told me, quietly, if you stay they'll give you one. So while the instructor and the whole group recited their texts, I sat at the back, face burning again.

"There was no meal after that. Instead, we worked in the garden. Work is good for you, said the matron to us, as she handed us a shovel, or a pick, or cutters. One of my itinerant jobs was gardening, so I knew immediately what to do, and I started pulling out weeds and trimming the grass edges. The matron came to me and told me to stand up. When I did, she slapped my face, hard.

"I dropped my shears in confusion. What was going on? All life is holy, she told me. How could you destroy those plants? They're weeds, I answered. Here, she said, nothing is a weed, no one is a weed. Not even you are a weed, though you are a miserable gardener. Plant them back, she said. So I spent an hour planting weeds. It was the strangest and most humiliating hour of my life, I think.

"By 10 PM or so, we were done and exhausted. Finally, food! It was boiled potatoes and some kind of meat stew. There were women sitting at the other end of the hall, all dressed in the same green-gray as the men. Some looked cute. It was hard to tell with those clothes and the hair all tied up in head scarfs. I felt out of place with my own clothes on.

"Sleep was a blessing. My mind was filled with unfamiliar feelings. What was this strange place, and who were these people? They seemed so calm, so peaceful. While part of me wanted to leave, to run away, I also felt a sense of security that I'd never felt before. No one is a weed here, the matron said. Not even me. Maybe for the first time in my life, I could belong.

Week Two: Bye-Bye, Mama

"Breakfast was the same, without eggs. Not a special day, I guess. Afterwards, an older man with white hair and a short white beard came to me and told me to follow him. He did not introduce himself, and we sat in a little room. He told me, be honest and open, and then asked why I had wanted to hurt the plants the other day. And then other questions about my feelings, my life, and so on. He smiled a lot at me with a twinkle in his eyes that made me feel comfortable and loved. We talked for so long. Only much later did I learn this was Father himself!

"One of my prized possessions is, no, *was*, a photo of my family, from a few years ago. My mom and dad, and sisters and older brother. On the back, their phone numbers scrawled in different pens. I wanted to call them, tell them I was OK, safe. Matron said I'd be allowed to do that in a while, maybe even in a few days. She asked to keep the photo for me, and said she would call my mother for me.

"Today I got chores, which was nice, because otherwise I'd have been bored and excluded again. Lunch was a vegetable stew. I missed my mother's cooking. She used to make such amazing meals! Roasted meats, fried vegetables, spicy sauces. As I ate that stew, I remembered it and started to cry.

"Matron came over and pulled me up, gently, and brought me into a room painted in bright colors. I sat on a wooden chair, one of about ten in a circle. After a while, other people came in, including some girls. Matron explained that I was new, and feeling lonely, and then everyone stood up and came and hugged me. I began crying again, and they hugged me more, and I felt myself almost faint from the intensity of the love.

"That afternoon, I told Matron I wanted to stay and would do anything necessary. She told me, good, hand over everything you have and we'll get you a proper set of clothes. I gave her the backpack with clothes and books in it, my old watch, and wallet. Then I went to get a haircut — close shave — and my clothes, my new name, and my num-

ber. I felt reborn, clean, perfect. Everything I had been, even my name, dead. A new man, a new life.

Week Three: A Brave New World

"Recitals, recitals, recitals. It's been weeks now and my mind is filled with the strangeness of it all. Words I never knew, concepts that attach to nothing except other slippery concepts. Enemies who want to destroy us, Father's fight to save us. First it's recitals, then it's tests. If we fail a test, we have to meditate in the silence room for a day, and then repeat the class. If we pass, we get accolades, and we move on.

"I was always a rapid learner and by now I've progressed well. One day on my knees in the silence room was enough! Matron says I'll go far. She smiles a lot at me these days. I can't believe I used to be afraid of her. I've already finished the First Book and passed all the tests with very high scores. At night, I read the Second Book and try to memorize it so that I can do better at recitals. I don't even know if there's a Third Book. People speak of it.

"Yesterday, my first punishment duty. There was a young woman, just a girl, who refused to eat her dinner. She threw it on the floor, shouting and screaming until she was taken away by three large men. The next morning, I was chosen to deliver Father's lesson. They didn't explain it to me, just took me to the room where she was being held, unlocked the metal door, and led me inside. She was tied to the bed, hands and feet, disrobed, gagged, face down. They told me, "Father says, do your will and you do His will. You have one hour," and left the room. I knew it was a test of my strength and faith.

"I would lie if I told you I didn't enjoy it. I wanted to remove her gag so I could hear her moan and cry. I didn't dare. I never saw her again. We rarely spoke or mixed with the women, so it doesn't mean anything. Perhaps she was on kitchen duty. She was so young. Does that matter?

"Tomorrow, they are choosing new people to go out for meetings. I've asked to be one of them. It's too soon, they tell me. At least I'm

now sleeping in a different room with fewer of us, and getting eggs every morning. Life is good. I wish my family could join us.

Week Four: The Enforcer

"Waking up every day at early hours for more recitals is hard. I understand the necessity for spiritual cleansing. Father showed us the way; we follow his steps.

"I finally got my own room. It's small, without any decoration, a little slit window and a concrete slab with a thin mattress for a bed. It has a door, and it's mine! They told me, the room is free because the last occupant did not love Father and we had to send him away. I don't ask what that means. I can guess. There are a lot of punishments here, some worse than others, and the very worst is to be kicked out, excluded, rejected.

"I know about the punishments because it has become my thing. I'm not sure why, they trust me with this, since that first girl. You know, they filmed it all, and later showed it to me. They record a lot here, on video. You'd think there were some secrets, some privacy. That's not true though. No secrets here.

"I have to admit a certain genius in inventing new punishments and applying them when people expect it least. There's nothing more fun than watching someone doing something they absolutely *know* is good, then pointing out that the rules changed, and that they are committing a terrible crime. Like stupid me with my weeds, that first day.

"Technically, everyone here is a criminal before we even start. Father says this many times in his recitals: we are all sinners, and only a few can be saved. The whole outside world, all sinners that want to destroy us. Most people here, sinners who will fail. Even me, a sinner, weak and filled with doubt. I know this, and every time I teach a lesson in blood or pain to another person here, it feels true and real again. 'Only through sin can we become truly innocent.' That's the first recital of Book Three.

"I think of it as a form of love."

From Bandits to Bakers

I trust you see from my story of the bandit Father and his gang of followers, that political movements, religions, and criminal movements of all kinds do not depend on the extremism of those involved. They are a form of prison. The overwhelming majority of people caught up in them — about 96%, to be precise[56] — are innocents who lack the very special talents needed to recognize what is going on from the start, and make what we could arguably call a choice.

Many of those trapped in such places adapt to survive and may become part of the system, yet they are doing what most of us would do. First, find a way to survive; second, rationalize what we have to do, or become. Whether it's working for a bank that is stealing pensions, or locking the doors on a labor camp, we need to find justifications.

Some countries do go crazy, yet most do not. What makes the difference? Highly motivated bandits are not a sufficient danger in themselves. They exist in every place and time, and mostly they can only do limited, local damage.

In order for bandits to get real power in a society and inflict wide scale harm to many[57], the social elements who would normally block this have to be too weak to act effectively. It's not random. Only specific kinds of people will really fight the bandits tooth and nail. And these people get their power and strength from certain conditions that are often externally defined.

I'm going to propose one more pop-science political theory, which is the "4B hypothesis." This emerged from my research into African politics and economics for "Magic Machines", and is as far as I can see

56 http://www.washingtonsblog.com/2012/08/as-many-as-12-million-americans-are-sociopaths.html

57 http://www.washingtonsblog.com/2012/07/why-dont-the-psychopaths-on-wall-street-and-in-d-c-show-remorse-for-their-destructive-actions-and-why-dont-we-stop-them.html

broadly applicable, a good tool for understanding broader political conflicts.

The 4B Hypothesis

For the sake of argument, let's divide society into four roughly equal chunks. We have the bandits, who specialize in taking from others, and who we have already met. Then, we have the beggars, who specialize in getting something for nothing. Middle management, perhaps. Then, we have the bureaucrats, who specialize in making rules and keeping things organized. Finally, we have the bakers, who specialize in making things that other people need.

There is both talent and opportunism. So, while some people are born to be a particular B, others switch depending on what works best. So you can have societies with 40% bandits, and societies with 10% bandits. And there are tipping points where suddenly whole generations switch from old strategies to new ones as times change.

Depending on various factors, one or other of the Bs will be in charge, aided by one or more of the other. By default, the bandits and the bureaucrats team up on the bakers, and ignore the beggars, who live in abject poverty. The only law is power and family. When the bakers — who after all feed everyone — begin to accumulate wealth and power, they slowly recruit the beggars and the bureaucrats into their ranks, and beat the bandits into a corner. As the bakers (the commercial middle class) get more power, they bring into existence what we'd consider the fabric of a modern state: stable currency, fair courts, representative government, commercial law, universal education, universal health, roads, water and food for all, housing for all, policing, and so on.

Let's work through the various possible states of society, depending on who's in charge, and map them to current societies:

- Bandits: Somalia, Syria (the bakers are on the run, and beggars).
- Bandits and beggars: North Korea
- Bandits and bureaucrats: United States, Italy

- Bandits and bakers: Russia
- Bandits, beggars, and bureaucrats: Zimbabwe
- Bandits, bureaucrats, and bakers: Saudi Arabia
- Beggars and bureaucrats: Cuba
- Beggars and bakers: Belgium
- Beggars, bureaucrats, and bakers: France
- Bureaucrats and bakers: Switzerland

The bakers haven't suddenly proven Darwin wrong and developed genes for altruism. They're acting totally selfishly, with a very different strategy from the bandits or beggars. The bakers need wealthy clients and stable suppliers. They need scale and growth, which transcends family and tribal ties. They need fair laws and courts to arbitrate, because conflict is bad for business. They need an educated workforce, and they need good infrastructure for transport so they can get their goods to market rapidly and safely. They need security. They need healthy neighbors because disease spreads.

The bakers need all these things because they are good for business. As the bakers and bureaucrats build a better society, the beggars help them, and all except the most inflexible bandits switch strategies and join in the boom.

Societies flip from state to state as they grow prosperous and develop a wealthy commercial middle class, exhaust resources, enter violent conflict with other societies, and so on. There is no inevitable path, just a set of states and events that push societies from state to state fairly predictably. Nothing here is new. Practically, the first written text was legal codes dating from 1,700 BC[58] and half of those cover contract law. Currency and banking date from 3,000 to 2,000 BC. Human society has been flipping between the 4B states since the dawn of history.

58 https://en.wikipedia.org/wiki/Code_of_Hammurabi

How Geography Drives Society

Now let's apply this hypothesis to different parts of the world. Bakers don't simply organize and get wealthy by being prettier and smarter. They organize around trade, which develops around two things: transport and markets. Initially, naturally occurring transport such as rivers, lakes, seas, and flat dry plains; and later, man-made transport such as canals, railways, roads, and airports. Markets mean cities, which means agriculture fed by fertile river deltas or plains.

The economy that develops in any region depends directly on the natural transport it offers. On the highly crinkly coastline of an inland sea, with hundreds of huge cities fed by rich farmlands, it is possible to produce and ship goods to millions of consumers. Large-scale trade, backed by military power, could build an empire out of a single city[59]. Large-scale economies build large-scale political systems, and large-scale baker-bureaucrat societies.

On the other hand, a jungle-covered country with no big cities and little in the way of natural transport will not develop a significant commercial middle class because there is no scope for trade. One can produce a thousand chairs, yet how to sell them, and who to sell them to? Societies that are isolated geographically and spread thinly over large landmasses do not develop industrial technologies: no glassware, no metallurgy, no precision instruments, no machines. At the same time, they don't develop advanced military weapons either. There is no need and no benefit in building warships in the middle of the desert, nor on an oceanic coast with no scope for trade.

As we look at the world, we see that the better the natural transport systems and hinterlands, the larger the population concentrations and the wealthier the society, and the more the bakers and bureaucrats dominate society. In Asia[60], Europe, America, and Africa, the most "developed" societies have always grown up around water, and the

59 https://en.wikipedia.org/wiki/Republic_of_Venice

60 http://www.zum.de/whkmla/histatlas/asia/haxasia.html

most "primitive" societies have always been the most distant from water. Compare Uzbekistan to Sweden, Texas to San Francisco, Chad to Uganda, Tibet to Taiwan.

The apparent exceptions prove the general rule. Switzerland is land-locked, nonetheless it derived great wealth from its position on the Rhine, its internal lakes, and as a crossing point for Alpine trade.

In fourteenth century Africa, the Manden Kurufaba empire of Mali controlled cross-Saharan trade in salt and gold carried on camels, or "ships of the desert." The Manden Kurufaba became so wealthy that when its king, Mansa Musa, traveled to Mecca, he spent so much gold that the price of the metal was depressed for a decade[61].

Post-genocide Rwanda, another exception, has a booming middle class and economy. There, it seems to be driven by the determination of the elites to never again allow such a horror to occur, with help from China and the US, and pillage from Congo-Kinshasa.

Northern civilization started in what is now Syria and Iraq, and spread east out to India, and west to the Mediterranean basin[62]. Without exception, the Mediterranean states, from prehistory until modern times, were based on maritime trade fed by major rivers and based around major cities.

So Europe was particularly rich in commercial middle classes who defended their precious institutions with blood. Over and over, as the bandits tried to gain power, the bakers drove them out. This may sound over-dramatic, yet the history of a country like France is basically one of bandits (the descendants of Vikings) being driven out[63] by coalitions of bakers and bureaucrats, using beggars as cannon fodder. And bearing baguettes, one imagines.

Conflict has been widespread throughout Europe wherever and for as long as there has been any significant population. And systematic-

---

61 https://en.wikipedia.org/wiki/Musa_I_of_Mali

62 https://en.wikipedia.org/wiki/History_of_the_Mediterranean_region

63 https://en.wikipedia.org/wiki/Hundred_Years'_War

ally, the baker coalitions have won. The last time the bandits were in charge in a European country was when Tito's Yugoslavia fell apart and bandits took over Serbia, then tried to conquer the rest of the region.

So Europe's current political models are a direct consequence of these conflicts. We learned, long ago, to look after the beggars and turn them into assets, not liabilities. We learned to create space for the bandits, giving them symbolic power in government. Belgium, my home, has a long history of commercial city-states fighting for their independence, and today has six governments[64]. To me, that's directly related.

Why and how do the bakers win? They need a few key things. Principally, they need freedom, and they need access to markets. When the bandits want to stop the bakers from taking power, their first tool is to block trade. Freedom can mean many things. My definition in "Freedom in Chains" is, "the ability to do interesting things with other people." And if you're a baker, that means to buy and sell, hire and fire, without undue taxes, tolls, delays, or theft.

Extraction Economies

When a country doesn't develop a commercial middle class, industrial technologies, a strong military, and strong institutions, it is particularly vulnerable to a certain form of theft that I call "extraction." This is when a bunch of foreigners land on your shores, buy up some local chiefs, chop down your forests, rip the minerals out of your soil, enslave a few generations, and eventually go home, leaving their half-caste bastards in charge.

If you're lucky enough to live in a malaria-infested swamp, the settlers leave or die. If you live in a healthy, inviting landscape, you will be corralled into reservations in the worst parts of the country (those furthest from water, of course). Your land will be taken away by "treaty." Your rebels will be slaughtered by machine gun, and the sur-

64 https://en.wikipedia.org/wiki/List_of_governments_in_Belgium

vivors poisoned with alcohol. And your prettiest women will be taken as concubines. After a few generations, people will forget you ever existed, except as quaint memories.

Extraction economies do not depend on a commercial middle class. There are no networks of trade. No one needs to read and write in order to carry rubies out of a deep mine. Educated middle classes make trouble. They form unions, elect honest politicians, and demand fair prices for their natural resources. Extraction economies don't just disregard the needs of the people; they actively oppress them. That is, for an extraction economy to operate at maximum efficiency, it must destroy the middle classes, and turn the mass of people into near-slaves.

When a land has limited resources, the extraction economy will stop. When the trees are chopped down, farms spring up; and farmers are just bakers with mud on their boots. However, if the soil is rich in valuable minerals, the extraction economy can continue for generations, even hundreds of years.

Fixing the Sick Men

Whereas analyses based on cultural differences, religion, skin color, or endemic disease do not offer much hope for fixing the sick men of the world, the 4B hypothesis does offer an answer. Moreover, it's something we see happening today, in real time, across Africa and much of the world. It offers us an answer to fixing the sick societies of the world. Give the bakers freedom and opportunity so they can form commercial middle classes and fix their own societies. Bakers do not need gifts: that just reinforces the beggars. Bakers don't need guns: that strengthens the bandits. Bakers need access to markets and the freedom to trade in them. In today's world, that means cheap, fast broadband.

Here's a claim: the quality of any society correlates directly to the performance/price ratio of broadband Internet in that country.

There is still one unanswered question. What is the best form of government for a country that has warring communities, no middle

class, and a history of violent politics? How does one solve a Haiti or a Congo-Kinshasa or an Angola? It seems painfully obvious that "elections" do not help, and have never helped. In these countries, the people are thinner and poorer than they were under previous dictatorships.

Fake democracy and dictatorship will have the same result: the looting of natural resources and the treasury, economic failure, suppression and flight of whatever remaining middle classes there are. There have been a few "gentle dictatorships" that actually promoted commerce and the middle classes. They are so rare we can consider them outliers. There was Tito's Yugoslavia, Venezuela under Chavez, perhaps China.

So what can the international community do when a country is unlucky? Would assassinating Hitler in 1929 have changed anything? The answer is no, it would have just created another martyr. Charismatic bandits are not that rare. How about foreign invasion and forced administration? It worked in Bosnia and failed in Haiti, Iraq, and Afghanistan. It's expensive, dangerous, and only makes sense as part of a smash-and-grab operation on the largest scale. It certainly doesn't fix broken countries.

I think the solution to fixing failed states like Congo-Kinshasa is to recognize that a government, whether "elected" or installed by violence or bluff, does not by itself create a valid state. When we recognize a failed state as a bandit gang, we see that the problem is the bandits and their economic model.

- The first step is to flag a country as sick when, like a person suffering from a mental disease, it becomes dysfunctional. We can measure that in terms of mortality and life expectancy, education, freedom of expression, and corruption.
- The second step is to accept a doctrine of international intervention. Just as we can demand that our neighbors be treated for infectious diseases, we can demand that sick countries be made

healthy again. It is bad for business and dangerous to have broken societies on your borders.

- The third step is to intervene by hitting the leadership of the country. They should be targeted personally and without pity. If they funnel assets out of the country, banks that accept such funds should be prosecuted. If they leave the country, they should be arrested and charged for crimes against humanity.
- The fourth step is to attack foreign businesses that are profiting from the situation. Anyone who sells them weapons should be prosecuted. Anyone who does business with the family of the leadership should be prosecuted. To change the behavior of an individual or a group, the only sustainable strategy is to change the economics. If it's unprofitable to be a thief, people will stop becoming thieves.
- And lastly, there should be strong pressure for cheap, fast, unfiltered broadband. This should be the main condition of the relaxation of pressure. High Internet costs and censorship should be treated as crimes against humanity, and access to IP packets as a basic human right, along with free education, clean water, and freedom to travel.

The reality is that we are still very far from this. The West has its own crises, its own bandits, and is immature in many ways. The next decades will be key. The violent racism that immigration provokes is a gold mine to politicians. The guilt and fear of getting too many chocolates, and eating them all, makes us northerners easy to mess with.

Will western society embrace multiculturalism, or turn against it? Will Europe one day allow black Africans to travel freely as we expect to do? Will the US one day treat Muslims and Latinos as equal to Protestants and Germans? Or are we heading to a world of global databases, ethnicity chips, and facial scanners at every railway station and bus stop?

At the heart is the question: Will digital society, which venerates diversity and multiculturalism, beat industrial society, which venerates paranoia and control? One can hope. It's far from inevitable. Those database and facial scanners are already there, and used 24/7.

Summing Up

In this chapter, we've looked at the ways in which the wise crowd can be turned upside-down to become a mad mob, and how classes seeking political or financial advantage often do this deliberately. In the worst cases, they create cult-like gangs around a core of bandits that can be extraordinarily destructive. Human social instincts, like knives, can be essential implements or deadly weapons.

Were the bandits always in charge or was there a big shift in the last decades? I think we're witnessing a shift, at least of perspective. It used to be so hard to know what was going on between the walls of power. Now like all our walls, those walls are getting transparent. And we're shocked, *shocked*, to see the nice old men we trusted all those years are just like, if not actually interchangeable with, drug wholesalers, loan sharks, and other miscellaneous mobsters. Wasn't corruption meant for poor countries?

The next chapters will look at three big areas where the old guard is fighting the new digital society. These areas are: freedom, privacy, and property. As so often, the real story is about people rather than technology, and it's cost gravity that drives the stories forward. Things get cheaper, and that shatters old assumptions and old arrangements.

Chapter 4. Freedom in Chains

Once upon a time, there was a great Empire that ruled the known world. It owned all the lands, the wealth beneath, and the wealth above. The Empire was run by an old, faceless society of criminals. It ran on cheap oil and cheap blood. It smashed its opponents in the name of Peace. It burned their lands in the name of Reconstruction. It enslaved them in the name of Freedom. It built massive castles of edict and punishment to govern its populations, and it fed them a river of pap to keep them docile. It was powerful, invincible, and paranoid.

Far away, in a different place, a civilization called Culture had taken seed and was growing. It owned little except a magic spell called Knowledge. The Culture ran on light, and built little bubbles of fire and hope. It seduced its critics by giving them what they wanted, no matter how unusual. And as it pulled in more people, it grew and built more of its bubbles.

When the Empire first encountered the Culture, it was puzzled. There were no armies to crush, no statesmen to corrupt and recruit, no castles to loot and burn. So it ignored the Culture and its pretty bubbles, hoping it would go away.

The Culture grew, and grew faster than you could follow. In less than a generation, it had started to build cities, impossibly beautiful spheres of fire and hope, massive, and yet gentler than the breeze. More people quietly left the castles to move to the cities of the Culture, where they too learned to build their own bubbles of flames and joy.

The Culture seemed harmless. However, the Empire depended on its vassal masses. If the masses left to go to the Culture's cities, the Empire would starve and die. Total War was inevitable.

Both the Empire and the Culture knew it, and prepared for it in very different ways.

The Empire attacked. It tore down the cities closest to it and told the Culture, stop building or we will come back. And for each city it burnt, a hundred others sprang up. Culture shrugged and said, "We enjoy building new cities." So the Empire sent its infiltrators and spies into the cities to try to corrupt them. And the Culture laughed, clapped its hands, and exclaimed, "We do much worse to ourselves every day. Look, we enjoy this game!" And it opened its hands. And there lay some of the Empire's darkest and deepest secrets, for all to see.

So the Empire, the cold finger of fear touching its heart, smiled its most sincere smile and welcomed the Culture into its lands. And then it began to erect a far wall so wide and so high that it could cover all the cities of the Culture in darkness. If the Culture ran on light, thought the Empire, then it would destroy light.

Defining Human Freedom

"Freedom" is a word we use a lot. I've used it two dozen times so far in this book. What does "freedom" actually mean to us humans?

The nineteenth century political philosopher, economist, and politician John Stuart Mill wrote in an unfinished late essay entitled "On Social Freedom"[65]: "*There is perhaps no question upon which it is possible to theorize to so little effect as upon the nature of human freedom*."

Most dictionaries define freedom by the absence of chains, real or virtual. "The power or right to act, speak, or think as one wants without hindrance or restraint," says Google. Like the dictionary definition, Mill's focus is on the individual and his right to either do

65 http://liberologi.wordpress.com/2011/10/01/on-social-freedom-by-john-stuart-mill/

something or not do something. This is fair, yet it begs the question of function. Why do we give such importance to these rights? To be brutal about it, what is the reproductive advantage of freedom? A chicken does not need to be free, so why does a person?

A wild animal needs freedom to find food and mate. Humans too need freedom, and we are a social species. Human freedom is, I claim, like human intelligence, more about the group than about the individual. This is a deeper meaning that the dictionary editors and political philosophers seem to have missed. Freedom is critical to digital society. The fight over freedom is not a small thing; it is one of our defining struggles. We have to be precise about *what* we're fighting for.

If you are alone on a planet with no walls or restraints or authority, are you truly free?

Most people will answer, "No, not really." The dictionaries are wrong by omission. Freedom is not so much about the lack of restraint as it is essentially about *other people*. Here is how I define freedom:

> *Freedom is being able to do interesting things with other people.*

This definition clearly includes the conventional definitions, and it also tells us why losing our freedom has such an impact on us as a social species. Without the freedom to do interesting things with other people, we are reduced to slavery.

The Cost of Subjugation

The uprisings in North Africa of 2012 and 2013 were of course about freedom. However, if you saw the TV interviews with ordinary people on the streets of Tunis and Cairo, they were ordinary middle-class people driven to desperation by poverty and lack of opportunity.

We have seen enough impoverished slave societies to accept that empirically, freedom makes us wealthier. Compare North Korea and South Korea, which were split in 1950 like identical twins raised by

very different families. Sixty years after starting from the same place, one of these countries is in ruins, while the other is a world success.

Freedom isn't the only differentiator, nonetheless it is the major one. Per capita GDP in South Korea is around $22,000. Accumulated over one lifetime, that values freedom in South Korea at about $1 million per person.

What kind of freedom are we talking about here? Mostly, when discussing freedom and wealth, people cite "economic freedom"[66] (the right to run a business, for instance, or own private property) as separate from "political freedom" (the right to create political parties, for instance, or stand for office).

The split can lead to strange arguments among those with strong political views. Take Friedrich Hayek, for example, who argued that economic freedom depends mainly on the rule of law and equality before the law. He continued, asserting that any "socialist" policy to reduce the gulf between rich and poor broke the principle of equality, and so would cause ruin.

Except, the opposite seemed to happen. Sweden, with its large public sector (and correspondingly less economic freedom), became much wealthier than the UK, which has a small public sector. Inequality and class divisions have high costs, as the UK car industry proved in the 1970's.

Someone should have stopped Hayek halfway through and told him, "Friedrich, dear chap, don't you realize there is no equality before the law? Rich men were never hanged, or deported to Australia. The law has *always* been a tool for the powerful. It's just that there are different kinds of powerful men. Some benefit from general poverty, and some benefit from general prosperity."

So the question is not: What kinds of policies are the men in charge enacting? It is, rather: What kind of men are in charge, and how did they get there?

---

66 https://en.wikipedia.org/wiki/Economic_freedom

I already tried to answer that in "Faceless Societies" when talking about the 4B hypothesis. Ludwig von Mises wrote, "The idea that political freedom can be preserved in the absence of economic freedom, and vice versa, is an illusion. Political freedom is the corollary of economic freedom. It is no accident that the age of capitalism became also the age of government by the people."

Political freedom seems to be a Catch-22. Without it, the bakers can't take power. Yet it's bakers, not bandits, who will create laws for political freedom. The way through the paradox is that some of those in charge are both bandits and bakers, depending on the situation.

All freedoms are different expressions of the same basic ability: to *do interesting things with other people*. There are many types of freedom, some much more basic than political or economic freedom. These freedoms support one another, and like bricks in a pillar, can be removed and softened individually without immediately bringing down the pillar — yet these removals will weaken the strength of the pillar to support a strong, resistant society.

Enemy of the State

The optimist, reading the past, sees our increasing freedom over time and predicts: in the future we will be freer than ever. The pessimist, reading the present, sees increasing clampdowns on freedom, and predicts: in the future we will all be slaves. The realist, reading past and present, observes: we only gain and keep freedom by fighting for it.

To fight for something requires strong fear or anger. Who in the West really believes we're losing freedoms today? We mostly have comfortable lives filled with gadgets, full fridges, and safe beds. Bad things tend to happen elsewhere, to other people. Who may or may not deserve it. We're enormously complacent, if not smug, and anyone who seriously claims the state is working hard to reduce our freedoms tends to be seen as paranoid.

However, while wealth and freedom correlate, full fridges and streaming TV shows do not equal freedom. Bread and circuses is a classic way to appease the people without giving them real freedom. We are so good at self-deceit, rationalization, and maintaining the sense of normalcy no matter how bizarre things get. "So far so good!" and "stop complaining!" fight for first place as the prime motto of the human race. Reality is badly out of focus to most individuals. We are easy to manipulate, and we are surrounded by propaganda.

It seems to me, observing this closely for more than a decade, that our governments are indeed working overtime to remove bricks in the freedom pillar. The process is slow, careful, and international. I think I've got a good explanation as to why they feel they have to do this, as told in my story at the start of the chapter, and I think that by now, the mechanisms are becoming clear to many other people too. A significant part of the process is to convince people that everything is normal. This plays on our desire to be relaxed and calm about things. When a person in authority tells us, "It's all OK," we want to believe them. When he's an out-and-out psychopath, it's even harder to resist that sincere smile and firm handshake.

In 2003, the US invaded Iraq, again, and between January 3 and April 12[67], 2003, 36 million people across the globe took part in almost 3,000 anti-war protests. In the US, however, the country actually sending soldiers to kill and be killed, protests were muted and small by comparison. This was, perhaps, at the height of power of the US propaganda machine personified by Fox News. That TV station has gotten quieter since Barack Obama's second term, when it bet so publicly on the wrong psychopath. However, that doesn't mean the propaganda went away. Instead it went underground, spread wider, and infiltrated our new digital media.

67 https://en.wikipedia.org/wiki/Protests_against_the_Iraq_War

I don't know how many government employees and contractors have fake accounts on sites like Reddit so they can try to influence what stories get reported, and how people respond to them. The sock puppets are there, that's a certainty, and it's something I'll return to later in this chapter. For now, let's examine how the classic propaganda media operated. These patterns seem to repeat fairly often, so I expect we'll see them come back in new clothes over and over:

- *Make false analogies*. Free speech is a human right. Companies are legal persons, and have human rights like persons. Supreme Court decision coming soon!
- *Promote a climate of fear*. Terrorists attempt to explode bombs on school bus. Justice Minister announces sweeping powers of detention without trial.
- *Think of the children*. Pedophiles are plotting to rape your children. Home Affairs Minister announces new censorship laws to protect your family from Internet porn.
- *Use circular reasoning*. Unlike those evil terrorists, we're a democracy. Everyone knows democracies are good. Therefore, your government is good. Elections are tomorrow!
- *Appeal to self-interest*. Ecologists want to raise the price of everything, so even if they might be right in theory, the market proves they are wrong.
- *Flatter by comparison*. President-for-life Smith of Eurasia is an evil dictator who eats children's hearts. And now, back to domestic politics.
- *Flood with useless data*. Wife of footballer confesses sex addiction, love affair with lesbian gardener. Now, back to the banking takeovers of this week.
- *Stir fear, uncertainty, and doubt*. Teenager arrested for anti-social on-line comments, facing terrorism charges and life imprisonment. Congress debates new security powers.

- *Debate empty emotional issues*. Should Muslims be allowed to write books about Christ? More coming up on this hot story after the news!
- *Create confusing terminology*. New report calls for harmonized integration of third-pillar powers, citing "inefficiencies" in criminal justice system. Download the full report now (registration required).

Of course, journalists and editors don't need to invent and insert these messages deliberately. They are as just gullible as anyone and can be manipulated in exactly the same ways. It just takes a few clever, well-placed people close to the top of the food chain, crafting wedge issues, talking points, and other propaganda elements. Feed these into the hierarchy, and they spread to the whole system.

As a note, I'm shocked that my "teenager arrested for antisocial on-line comments, facing terrorism charges" line actually came true in 2013, multiple times. I wrote it several years ago as an absurd caricature.

Kisses in the Park

> *"According to a Sydney Morning Herald article, the Australia government has decided to take the controversial step of having Internet service providers filter web content at the request of parents, in a crackdown on on-line bad language, pornography and child sex predators."—Slashdot front page, 9 August 2007*

Having our thoughts held captive under the influence of propaganda only lasts for so long. We eventually clear our minds and realize that things are not quite right. For longer-lasting results, the men in charge have a more solid argument against freedom. I'm not talking about terrorism. I'm talking about simple morality. When people have too much freedom, the argument goes, they do bad things. Therefore, we will make laws For Everyone's Own Good that make those bad things illegal.

Morality and law-making often walk hand-in-hand, and they make an unpleasant couple. Legislators are powerful men (and rarely, women) who have worked for years to acquire that power, no matter what the cost.

Individuals with such power over others tend to see themselves as free of the constraints of normality. This superiority complex is made worse by the psychopathy that many men in power are afflicted with. We regularly discover politicians selling their votes and influence, receiving bribes, colluding with gangsters, seducing young pages, buying and selling drugs. Their reaction is typically one of regret at getting caught, with a promise to do better in future. And the public reaction? "So, what's new?"

Indeed, such behavior is almost the rule, in politics the world over. In some countries, politicians revel in the infamy of their behavior. "The laws do not apply to us," they say, and vote themselves parliamentary immunity and pay increases. A man or woman who is constrained by a strong sense of ethics does not survive the political process. So it's nastily ironic when men and women fight their way to office, over the bodies of their political opponents and the bones of social norms, and then create laws that regulate the ethical personal behavior of others.

In the Middle East, the soldiers and priests still have a firm grip on most countries. Iran, one state on the verge of a middle class revolution after the fall of the Shah, became imprisoned in an iron blanket of moral legislation. In Iran as in Afghanistan, every behavior is either illegal, or obligatory. These are classic cult techniques, as we saw in "Faceless Societies". Thus, the correct explanation for mad mullahs who string up and stone women and men for the least misdemeanor is not, "Muslims are dangerous." It is, "cults are dangerous." The same can be said of suicide bombers in other contexts.

In the West, we escape the type of virulent moral legislation that infects countries like Iran, Saudi Arabia, or even Dubai. We don't arrest women for walking alone, and we don't usually beat up teenagers who kiss in the park. We don't usually jail or murder women for being raped, yet we do regulate lots of different types of behavior:

- Most countries have draconian anti-drug policies. The usual justification is public health, yet anti-drug legislation does not actually make the public healthier; it tends to raise the profit margins of gangs and criminal elites.
- Suicide and euthanasia are illegal in most countries, even those that employ the death sentence. It seems that only the State or natural causes are allowed to decide when or how we die.
- Homosexuality is no longer illegal in developed countries, yet only a handful give same-sex marriages the same weight as male-female marriages. Many people may have prejudices about "gay marriage." Why should the State express these prejudices through law?
- Forms of pornography and commercial sex, abortion, and various forms of sexual activity between consenting adults are forbidden or heavily regulated in many countries. Why should the State regulate our sexual behavior even in the case of consenting adults?
- Gambling is illegal or heavily regulated in almost all countries. This is usually defended because gambling can be so destructive to families, yet banning or regulating gambling does not stop gamblers, just as the ravages on families of drug addiction are not ended by making drugs illegal.

The claims that such prohibition laws exist to help the people do not really hold water. When politicians pass moral legislation, they do it for because they think it will help to keep them in a position of privilege and power for a little while longer. These laws act as political tools with a common purpose to reduce and diminish our social freedoms whilst protecting those in power from responsibility for social problems. They turn us into a potential criminal majority, all pos-

sibly guilty, all the time, of various crimes, and all potentially targeted for arrest and sentencing on the grounds of our moral lack.

Once the State claims the right to suppress social freedoms for our own sake, the side effects can be dramatic. We don't have to look at the Persian Gulf states to see examples. In 2013, for instance, Florida abruptly shut down all Internet cafés under legislation to stop on-line gambling. Was the goal to stop people betting, or to experiment with how people would respond to a ban on anonymous Internet access? If it was the latter, we may soon see other states across the US enact similar bans.

The War on Drugs created a boom for the security industry, and provided cover for a huge program of militarizing the police. It gave them the tools for citywide surveillance and rapid armed response. The story that the police exist to protect good people from criminals sounds more and more like a fairy tale.

For a long time, perhaps since the United States was founded, minorities have understood the police's role is to bully the poor on behalf of the wealthy. This view is now mainstream, particularly when civil seizures of land and property[68] started to supplement police department budgets. The differences between Kinshasa and downtown Los Angeles are not always as hard and fast as they may appear.

The Modern Police State

The program of arming the police went into overdrive after September 11th, when all restraint and budget control was thrown overboard. Men with guns don't care whether they're arresting someone for infringing on a drug law, or for infringing a law on sedition. The creation of a standing force — armed and trained and in every urban center — may seem pointless and wasteful, yet if you're a wealthy white male looking with paranoia at the end of your regime, it makes perfect sense.

---

68 http://www.businessinsider.com/how-scary-drug-raids-became-a-cash-cow-for-americas-police-2013-7

Late in 2011, there was a nationwide crackdown[69] on the Occupy Wall Street protests that gave us a demonstration of this new power. It's a story that you might expect from China, Egypt, or Russia, and it happened in the "Land of the Free." In the Guardian, a remnant of old media that has made its specialty out of reporting the politically difficult news others won't touch, Naomi Wolf wrote[70]:

> *It was more sophisticated than we had imagined: new documents show that the violent crackdown on Occupy last fall — so mystifying at the time — was not just coordinated at the level of the FBI, the Department of Homeland Security, and local police. The crackdown, which involved, as you may recall, violent arrests, group disruption, canister missiles to the skulls of protesters, people held in handcuffs so tight they were injured, people held in bondage till they were forced to wet or soil themselves — was coordinated with the big banks themselves.*

There are so many shocking aspects about this story. Not least of all is why the American media mostly ignored it, and how the few journalists covering the crackdown were removed by force and even beaten up[71] by the police. Also how the entire US internal security apparatus seems to be at the beck and call of the rich and powerful, in real time. The coordinated attacks on Occupy Wall Street — including a media blitz that successfully painted them as dirty, disorganized, wastrel hippies with nothing to say — started even before the protests took shape.

Naomi Wolf's explanation was, "follow the money." Occupy Wall Street was mainly a protest against corruption, and since the US government is filled with corrupt men, it was logical that the response to

---

69 https://www.google.com/search?q=ows+crackdown

70 http://www.guardian.co.uk/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy

71 http://www.guardian.co.uk/commentisfree/cifamerica/2011/nov/25/shocking-truth-about-crackdown-occupy

protesters from the State would be more brutal and broadly coordinated than usual. That seems to make sense. Yet we may also have to wonder how that massive internal security apparatus was so conveniently ready and waiting.

Perhaps the saddest thing about the events around the ending of the Occupy movement in the US was that most of America simply did not care enough to respond. The beatings and arrests of ordinary young people peacefully protesting against political corruption should, in any normal circumstances, provoke outrage. And that outrage should have amplified the protests, and turned them into a much wider set of confrontations in defense of the anti-corruption movement. Instead we were treated to a visual slapstick comedy of cops pepper-spraying dirty hippies on the sidewalk, and the public started to disassociate themselves from the victims.

America has problems, and they are not simply the corruption of the ruling class and the evisceration of the middle class. One of its most profound problems is the lack of old and deep relationships between most people due to a history of immigration, a culture of internal migration, and an old division between rich and poor that creates strong negative emotions on all sides.

The thinness of relationships manifests itself both on the individual micro and the national macro levels as both easy openness to strangers, and distrust of them. Americans seem to show a capacity for sharp and hostile responses to real or imagined threats, a disregard for others' suffering and cost, and an emotional view of the world, driven by lust, fear, hate, jealousy, anger, and self-pity. Working in many countries, often with difficult cultures, I've sometimes thought that cultural differences could be caricatured as personality disorders. The US has quite the collection.

The bright light is — as it is so often — the social media-connected youth, who are learning and building a very different culture, one based, for the most part, on equality, tolerance, positivity, and a bal-

anced, less emotionally defensive, and more creative response to threats.

The Elementary Freedoms

"Doing interesting things with other people" covers a lot of ground. Let's take it in the order I proposed in my preface to this book. First, we organize socially. Then, we organize economically. Finally, we organize politically. It's not a straight line. Our activities cycle back into each other over and over, little bubbles of fire and hope that cluster together to build whole cities.

We've discussed social, economic, and political freedoms. I'll come to privacy and property, which are often mixed into the concepts of social and economic freedom in "Eyes of the Spider" and "Wealth of Nations". While these major freedoms are the ones we see and talk about the most, I think there are four elementary freedoms, on which all other freedoms are built.

These elementary freedoms are:

- *to participate in a society*, including the freedom to leave.
- *to organize with others* and build relationships with them.
- *to know what is happening in society* and the wider world.
- *to share this knowledge with others*, without restriction.

The freedom to participate defines our relationship with society. It lets us choose our authority, and negotiate better rules by the threat of leaving if the rules don't work. Societies need rules, and the rules must be sane. There's no absolute, universal rulebook, so societies must adapt rules that relate to the real or virtual territories they inhabit.

The freedom to organize defines our relationship with other individuals. Relationships can be based on sharing knowledge, work, time, problems, and so on. This freedom must be moderated by ethics, which I see as a balance of power between parties. A relationship is ethical only when established by mutual informed consent.

The freedom to know defines our relationship with wider reality. More accurate knowledge lets us make better decisions. Knowledge of others' secrets can be ethical only when it is mutual. I don't mind people spying on me, in fact I'll defend that freedom, on the sole condition that I can spy equally on them.

And the freedom to share defines how efficiently our collective intelligence works. The greatest threat to the Internet, and the pet hate of most of its users, which moves them to action no matter the cost, is censorship.

You may recognize that these four freedoms as the core of the Social Architecture toolkit, and this is no coincidence. On-line communities have distilled the fermenting old world societies into a purer, more potent, and addictive form. If you look at successful on-line communities like Wikipedia, Twitter, or Facebook, they express precisely these four freedoms. To some, these distilled digital societies may seem artificial and unrealistic — even antisocial. However, they are actually hyperreal and hypersocial.

Next I'll examine each of the elementary freedoms in detail.

Freedom of Participation

After narrowly not escaping military service in Belgium in 1984, I lived for 15 years in the city of Antwerp, and then moved, quite randomly, to Brussels. That turns out to be a very different city and culture, tolerant of diversity and relaxed in its attitudes to the unknown. By contrast, Antwerp epitomizes the small-minded fear and hate of the poor by the wealthy. The city suffered massive flight of the middle classes in the last century to suburban homes and malls, and its downtown resembles urban blight covered with multiple layers of cheap, peeling paint.

Brussels, on the other hand, consists of 90% or more of immigrants, who have filled every corner of the city with life and noise. It's also dirty and poor, yet new activity springs up everywhere. No part of the downtown is safe from the hipster designers and art galleries

and little shops, above all, bars and cafés and restaurants of every color and style.

Not only is it a very mixed city, its population fuses together with an in-your-face glee. It's a people that has largely agreed to discard its culture and mixing taboos. Flemish nationalism and Islam still hold strong in some districts, yet they are both losing to the sheer pleasures of multicultural life. In no other city have I seen young North African women wearing full head scarfs, along with tight jeans and high heels, speaking Dutch to each other and French to their parents.

While I like a lot about Brussels, that isn't the point of this book. The point is that I felt free as a young man to move to this city, and to build a life here despite having no job, and knowing no one. The freedom to move to Brussels is one I took utterly for granted. It wasn't always so. Belgium used to be a cluster of city-states in which the right to live within a city wall, to be a free man of the city, and to enjoy the security and prosperity that living in town allowed, was restricted to elites.

The walls around our medieval cities weren't entirely against warring invaders. They were also against peasants in the fields who got tired of spreading pig trots and pulling out cabbages and yearned for a better life in the city. Yet those walls became symbols of the past because we learned that without streams of peasants abandoning their fields and their pigs and cattle, our cities would never prosper or compete.

Immigration looks set to remain one of the great debates of the next hundred years or so, and the outcome will reflect history. Eventually it is likely that we'll all have to be allowed to be free to travel anywhere in our world without interference or pressure. It's true that I was asked for my papers when I moved to Brussels, so I could register my address and pay my taxes. One of the legacies of Napoleonic and Roman law. But there was never a question about my *right* to be there.

The walls didn't all come down in the seventeenth and eighteenth centuries, of course. Some walls remained until the late twentieth century, and many walls remain today. When my wife and I married, she was an immigrant from Congo-Kinshasa and I learned just how difficult it was to cross the wall from Africa to Europe. Dear reader, you are most likely similar to me: white, western, northern, and accustomed to traveling anywhere in the world without much trouble. Perhaps you need a visa or two, though they are not trouble to get. Well, the sheer height and slipperiness of the wall facing the poor, dark, imprisoned south would shock you.

The reason for the walls around our old cities was to protect the privilege of the few against the many. Also, yes, for defense against bandits and raiders and the random foreign army. Yet how much of that history is true, and how much was just repeated as the excuse for taxing the burghers in order to raise the walls?

By the old definition, anyone who really wants power is going to be in trouble when they get it. Rulers in every time and place have started with the best intentions and end up shooting for Dictator for Life. It's just how it goes. However, there are checks and balances: crazy rulers are bad for business, so they tend to come to colorful ends. Still, sometimes you just can't fix a place and the only solution for the smart middle class is to leave for somewhere else.

In the sixteenth century, the Spanish found themselves in Flanders with a wide rebellion — Spanish classes sucked, presumably — and tried to fix that by looting and burning every city[72] in the region. The Sacking of Antwerp in 1567 was particularly destructive, with over 7,000 citizens of the city killed along with uncounted refugees.

Perhaps this is why Antwerp is still so miserable today. It's a fair excuse. The other cities that were burned by the Spanish — Aalst, Mechelen, Maastricht — all have that similar things-were-so-good-in-the-early-sixteenth-century whiff about them. Yet Antwerp used to be the center of the Netherlands in every way:

72 https://en.wikipedia.org/wiki/Spanish_Fury

rich, powerful, cultured. What happened? Possibly, as the Spanish worked their way across the landscape over several years, every smart and mobile Dutch speaker moved north, out of the way. It was literally just a matter of hopping into a boat and floating downstream on the Schelde River. You don't even need to row or steer. By the time they came to Antwerp, only the immobile or suicidally stubborn were left.

This mass northwards emigration kick-started the Renaissance in the Netherlands, which for a long time was a beacon of tolerance and enlightenment in Europe. It's also, incidentally, one reason the Flemish still distrust French speakers, who sided with the Spanish. The older the blood, the harder it is to wash it off. I'm half Scottish, and 500 years later, we Gaels *still* don't trust anyone with an English surname. I'm watching you, Mr. Smith!

The freedom to walk away is an ancient one; it's how we humans covered the edible planet. Every time there was a blood conflict in a village or town, one faction picked up its stuff and walked away, cursing and spitting over their shoulders, and secretly happy they didn't have to clean up the mess. I'd guess it took less than a thousand years to tramp around the whole globe like this.

Because people are essentially valuable, when they walk away, you have a problem. If most people living in Antwerp felt like me, and moved to Brussels, it wouldn't make the few remaining in Antwerp immensely wealthy and those in Brussels incredibly poor. Quite the opposite: Brussels would explode with activity and new wealth, while Antwerp would fall into abandon and neglect, just as it did in 1568.

So what we get is grudging competition between authorities to make people happy. The fewer walls, the more competition, and the better the overall results. Even if you assume authorities are innocent yet somewhat incompetent (rather than malicious and utterly evil), people walking in or out is the only way they can measure how well they are doing. How is it then, that in the twenty-first century, we still

accept national borders when we've long ago discarded our city walls? What is the cost, and how will this change over the next decades?

The enduring strength of the nation-state is partly the inheritance of history, partly the opportunism of power. Even in places like much of Africa where the boundaries of states make absolutely no logical sense, once a line is drawn and blood is spilled over it, it becomes a fact. Eventually the nation-state will become an anachronism like the city-state. Despite a few holdouts, the world will move slowly to a very different model of organization. I've no idea what that would look like. It will depend so much on things that are invisible today, particularly the deflation of old industrial-age power systems and the creation of new digital ones. The old lines won't be erased in one act, they will fade slowly, and unremarked except by historians, into insignificance.

One of the happy things about the Internet is the freedom to walk away. If our favorite forum suddenly bans picture posts and if we're sufficiently annoyed, we simply walk away and start a new one. When a forum loses its members, it will, like the Spanish Netherlands, sink into irrelevance.

Here are some predictions:

- An increasing global competition for talent. Simply put, as people come on-line, the competition between talented people increases in volume and effect. Today, already, we think nothing of recruiting designers from Malaysia, engineers from South Africa, project managers from Germany, and then bringing them together with a team based in Israel. So for at least a section of global society, business will demand — and get — easier migration.
- The need to attract young blood as the population of a country starts to age. It's the elephant in every developed country's living room. As more women go to higher education and full-time careers, they delay their fertility and so there are fewer babies. It's pretty simple math: 2 + 0 = 2. Most societies won't tolerate the Taliban solution: namely, banning education for girls. The other

two options are industrial-scale cloning, and allowing more immigrants.

- The dismantling of barriers to immigration and the promotion of pro-immigration policies, starting with an embrace of economic migrants (who presumably represent the most valuable newcomers), and moving to a general "open borders" policy much as the UK did with migrants from Eastern Europe in the years before the last recession.

One country to watch is Australia, which sits on huge natural resources, yet has too few people. Predictably, wealthy Australian society has become hostile to the poor people who attempt to settle there. It's the same story of too many chocolates: guilt and fear. At some point, unless it welcomes newcomers while it can, Australia will find itself barren, the iron and coal gone, and the cities dying.

The UN thinks the world will hit peak population by 2030 or so. Interestingly, this estimate has been dropping, from 2100, 2080, and 2050. It seems to me that this will trail Internet connectivity quite closely. Since that has exploded faster than anyone expected, we may hit peak population even earlier.

At whatever point we do hit peak population, the developed world will already have been experiencing falling birth rates for some time, and will be competing explicitly for immigrants. Initially, the cream of the crop, then later, the bar will fall. Politicians and media are already shaping public opinion to accept more foreign immigrants.

So that's my timetable for the sea change in public perception of immigration and subsequent changes in law to make it much easier for those able to pay the airfare to move to a better country. The key part is that emigrants have a choice, so countries will have to compete. And the main criteria won't be standard of living or climate or dominant religion or cuisine. It will be quality of government. If you were leaving the Spanish Netherlands of 2030, metaphorically speaking, would you go to a country with more or less freedom?

Freedom of Organization

> *Azmeen said: "Although I'm a Linux person, I must say that yeah, Microsoft does receive a lot of stick from us open source folks. Of course, MS do get a lot of things right at least in the technological and UI aspects." — Microsoft sock puppet on Slashdot, February 2008*

As I explained in "Faceless Societies", human society in all its richness can be seen as a truth-mining machine. There are of course many kinds of truths in addition to the physical facts for which science searches. For example, there are truths about problems, such as: "Congress is going to pass a bill that will allow censorship of any website." There are truths about solutions, such as: "Emailing your congressman won't help; call him or send a paper letter, or better still, try to visit him." And then there are truths about ourselves, such as: "Most people would rather chat about movie stars than engage in politics."

We extract truths by filtering, like whale sharks, interesting nuggets from the sea of information in which we swim. We then share these nuggets, and we debate them. Over time, this produces more accurate truths, which we continue to share by writing them down and providing that to others. We're pretty good at this, and especially at building tools to automate the process for us. We don't, generally, suffer from information overload.

Our social networks are just such tools, despite early notions that they mapped our "relationships." We'll talk to anyone who will listen, and listen to anyone who sounds interesting. When a "relationship" exists simply because someone clicked *Follow* or *Like*, it's really not the same type of "relationship" we were talking about. It's something else.

So it was quite predictable that Facebook and Twitter would become the first platforms for protests and then for outright revolutions. When this first started in the 2009-2010 Iranian elections, it

took governments by surprise. Perhaps until then, they'd believed that people were just sharing photos of their kids and pets. More likely, the old men who hold power around the world simply had not started using these tools, and had a slower learning curve than most other people. Barack Obama's election campaign heightened politicians' awareness worldwide of the potential benefits of using social media, though not everyone caught the bug.

Facebook and Twitter are a little passé today. For one thing, they are vulnerable to censorship and worse. Post a threatening tweet, even jokingly, and you will be arrested, as many people have learned[73]. The state security services are rich in everything — except a sense of humor. Today, the state of the art for on-line organization is Anonymous, with its (still somewhat naive) "You don't know who I am, so you can't arrest me" attitude.

Real communities spread far wider than the websites we visit. It was not a Facebook revolution, it was an Internet revolution. It is becoming clear to all sides that the primary challenge to the naked villainy of traditional politics is this new on-line society and its activist communities being able to arrange for 'real time' events through on-line communications; in other words, being able to organize themselves..

The real-world protests we see emerging in cities around the world are not random. In Rio today and tomorrow in Glasgow, these are not chaotic events driven by local crises or city politics. They are the fruits of an unseen global network, like mushrooms emerging through the forest floor. For every individual who went to an Occupy Wall Street event, tens of thousands took part on line, even if their involvement was limited to sharing photos of some event.

So the challenge for the industrial political elite is how to map and understand these networks, and how to control them or break them. Some dream of banning the Internet, yet that would be like switching

73 https://www.google.com/search?q=arrested+for+posting+tweet

off the power grid. When the Egyptian regime in fact tried this in 2011[74], it only intensified protests. It did not stop them.

Nationwide firewalls are another "cut off your nose to spite your face" strategy. Iran is currently trying to force its population to use a completely fenced-off Internet, going as far as mandating a single email address for everyone. Presumably, this is because — unlike the US government — they can't spy on Gmail.

China has censored its Internet access for a long time, however that filter is leaky, and has to be. If you actually cut your citizens off from the outside world, they can't do business, and your economy will suffer. This is the North Korea option, which only really works in an already poor country. Any interference in the smooth running of the global Internet would bring the wrath of big money down on the hapless idiot who tried it.

Let's look at some other strategies that different authorities are using[75] to weaken or reduce our freedom to organize on line without being too obvious about it:

- *An emerging censorship*, usually on the basis of child pornography, obscenity, terrorism, or copyright and trademark violations. There are different approaches. Among developed countries, Australia and South Korea (to my knowledge) maintain blacklists of websites that Internet users cannot access. These were pushed to "save the children": an easy sell to certain kinds of adults. In both cases, the blacklists grew wider and wider.
- *Manipulation of content*, where "sock puppet" contributors repeat disinformation, down-vote accurate stories, and up-vote their colleagues' lies. This is an old tactic that was first used by businesses like Microsoft who tried very hard to spread their view of reality across popular geek sites like Wikipedia by paying people to blog in their favor.

74 http://gizmodo.com/5746121/how-egypt-turned-off-the-internet

75 https://en.wikipedia.org/wiki/Internet_censorship_by_country

- *Fear and uncertainty*, where individuals are arrested for specific activities that may be more or less innocent. Laws originally designed to protect children from sexual predators now mark children as "sex offenders" for sending each other nude "selfies."
- *Removal of privacy*, where the State makes it clear that it is listening to our conversations, and takes them very seriously. The arrest of more than one teenager[76] for making sarcastic threats inside an on-line video game sends a clear message: we're watching, so behave.
- *Agents provocateurs*, where specific communities or projects are infiltrated by agents who try to push participants towards violent acts or words, so they can be arrested or subverted. This happens in many real-world protests, as police forces have an economic incentive in more, not less, disturbances.

Any experienced activist will assume that most large Internet firms, indeed most large technology firms, are tied into the surveillance networks, and collaborate with the alphabet agencies in varying degrees. That includes phone companies like Verizon, broadband providers like Comcast, major commercial websites like Facebook, Twitter, and Ebay, software firms like Microsoft and Oracle, network equipment providers like Cisco, and so on.

Large Internet firms claim to resist pressure to collaborate with the alphabet agencies. It would, however, be naive to assume that statements such as, "We do not give the National Security Agency access to our servers" are not lies by omission. If an agency has full access to the networks, it doesn't need access to servers. If the NSA isn't listening, perhaps others are.

Power must use a delicate hand when interfering with our ability to organize via the Internet. The Thai military has squadrons of soldiers whose job it is to write flattering comments about the country's monarchy, and down-vote criticism. The Chinese army does the same with

76 http://dailycaller.com/2013/07/02/second-teen-spends-months-in-jail-for-video-game-threat/

political discussion on forums. It's a little comedic because of course no one going to such a forum will be swayed by thousands of obviously insincere comments (or even sincere ones); they go to argue.

I assume that western spies are a little more sophisticated than the Thai military, and aren't simply spamming the Web with comments about how great the US political system is. What the spy state wants is to know everything about everyone, now, and provide this to the security services so that they can suppress or divert political dissent.

To reach this goal of "Total Information Awareness," society must use the Internet more, not less. We have to trust the websites we visit and trust our personal lives to, otherwise it becomes too hard to spy on us. We have to feel safe enough to expose ourselves, otherwise we'll find ways to hide. The cat, hunting a mouse, must wait silently until the mouse feels confident enough to leave its hole. Only then can it pounce. The spy state is the cat and we are, in its eyes, the mice.

If enough people feel annoyed by state surveillance, it's quite plausible that the leading edge of digital society will move to fully private forums running on private darknets. If this were to get any kind of weight and the mass market were to follow, it would present a real problem for the state security services.

Here is how I think this game will play out:

- As whistle blowers leak information about illegal spying by the alphabet agencies, we'll see denials by business and promises by governments to roll back such activities or limit them to extreme cases. Those denials and promises will be empty.
- In order to build more accurate on-line profiles, we'll see "real name" policies by websites and legislation by countries that make it illegal to use aliases in on-line communities or communicate anonymously.
- We'll see various forms of attack on anonymous communities, covering the gamut of negative media reports, planting illicit material, claims of infiltration by security agents, and so on.

- We'll see various attacks on advanced cryptography, possibly through patents, or through laws that mandate the use of algorithms sanctioned by the NSA. If you want to do business with the Federal government, you will use such and such algorithms. This won't stop experts, though it would slow down mass adoption of secure systems.
- If Reddit or 4chan or any other major community starts to organize fully private forums using modern cryptography, they will be sold to better owners who will stop it, citing technical difficulties, child porn, or other reasons.

An escalation of the fight between free political speech and censorship seems inevitable, and I think the outcome will mirror the older fight against file sharing. That is, we'll move away from centralized services accessed over commercial broadband — both easy targets for the authorities — and towards distributed services accessed by local networks, wrapped in unbreakable encryption.

Some file sharers used to make the claim that sharing music, TV shows, and movies was a form of political free speech. It seems that this claim wasn't wrong, just premature.

Freedom of Knowledge

In 2007, when Congress asked for documents relating to the dismissal of eight US attorneys, it turned out that the Bush administration had been circumventing the Presidential Records Act[77] by using an external email server (gwb43.com, run by the Republican National Committee) for sensitive emails. Over 80 senior staff used accounts on this server for official business. All the email for more than 50 of these accounts was deleted. The 2009 estimate of lost emails was a staggering 22 million.

In effect, the internal records of two of the most controversial presidencies ever were deleted by the president's own staff. The adage, "If you have nothing to hide, you have nothing to fear" could not be

77 https://en.wikipedia.org/wiki/Bush_White_House_email_controversy

more apt. No prosecutions were ever launched against anyone in the Bush administration for this (or anything else they did during those eight years). Wiping out these records was a major crime against the public interest, yet it was hardly unique. The Bush regime was just unusually innovative and blatant.

The gwb43.com email server was a form of "digital sandbox," a place to conduct business privately and then wipe it all clean, erasing all traces and accountability. Creating digital sandboxes has become very cheap, so their existence is now a fact of life. Digital sandboxes are not actually secure because they are accessed through the normal Internet, which makes them vulnerable to wiretapping. Most likely, because crooks rarely trust each other, those 22 million emails sit somewhere on a USB stick or tape waiting to be leaked.

To create a truly private sandbox, you need a totally separate network with no Internet connections at all. We call this a "darknet" (dark network). Darknets are used by people who *really* cannot afford for their communications to be tracked. Military-grade darknets have existed for decades. These networks are entirely separate. The computers in them do not have USB drives, and you cannot install software on them. They are completely secure. We can logically assume that governments are moving to military-grade dark networks for business that they want to keep out of the history books.

In November 2007, Enron collapsed in an implosion of financial chicanery, pension fraud, and cover-ups. One of the president's best friends even went to jail. That was an extraordinary event even then, let alone today, and makes me wonder who he crossed. Enron used financial bluff and lies to hugely overvalue its business, which gave it control over the energy market. It used that control to push for deregulation so it could buy cheap and sell high. Enron's aggressive manipulation of the markets caused such instability that California, the wealthiest region in the world, was hit by rolling power cuts. Enron then falsified its accounts to hide its gambling, and stole from its own employees when its losses got too large.

My surprise at the time was not that Enron went belly-up; it was that more firms did not follow suit. Of course, when the financial crisis hit in 2009, the world discovered that such practices were mainstream, particularly in the financial markets. As with Enron, the lack of oversight by regulators and transparency for shareholders were big factors in the worst excesses.

Large businesses, like crooked administrations, like secrecy for many reasons:

- *To hide financial delinquency.* Many firms routinely shift funds to and from subsidiaries, over- or undervalue assets, overcharge for internal services, use risky financial instruments to back debt, gamble with exchange rates, and so on. Such acts would not make the market, regulators, or taxman happy if they found out about them.
- *To hide unethical behavior.* Manipulating nicotine levels in cigarettes, lending money to dictators to conduct genocides, conducting dangerous product trials on uninformed test subjects, using child labor, buying black-market materials, polluting rivers, stealing pension funds, bribing politicians, muffling union organizers, and so on. As with financial delinquency, profits can suffer when such acts become public knowledge.
- *To hide internal corruption.* Directors, with the right to set their own salaries and benefits, regularly stretch the limits of what is appropriate. When confronted by unhappy shareholders, the response is usually, "Those are standard market practices," meaning "Everyone else is cheating their shareholders, so why shouldn't we?" It's much easier to keep such acts secret.

In all cases, we have conflicts of interest between a privileged group with its hands on the levers of power and wider society. We see that transparency would force a change of behavior and loss of profits. Secrecy is good for the bottom line and it keeps you out of prison, as gwb43.com proved.

Businesses have used lots of techniques to keep their internal records away from public scrutiny. Here's a sample:

- *Arguing that a company is a person with the right to privacy.* The bizarre notion that a business is a person was made law by the US Supreme Court in the infamous Citizens United decision of 2010. This was one of the main complaints of Occupy Wall Street (OWS). Of course a business — and I own several, I should know — is just a proxy for its shareholders. I've even had lobbyists lecture me that companies come under the UN Declaration of Human Rights.
- *The use of private equity to take firms off the markets* and out of the regulator's watch. Stock markets are efficient at allocating capital, and they demand certain reporting standards from firms. Private equity buyouts solve the shareholder issue and enable firms to operate within a wall of secrecy. The growing trend of private equity buyouts raises two main questions. First, where does all this money come from? Second, what is the economic benefit of the buyouts, except secrecy?
- *The use of regulation to plug leaks.* Primarily, this refers to the US Sarbannes-Oxley Act of 2000 (SOX), which mandates the recording of all electronic communications for larger firms. While this sounds like a good thing, my cynical brain experienced SOX while working for JPMorgan Chase & Co. I noticed that its main effect was to switch off all "unofficial" routes to the outside world. Under SOX, firms allow only monitored email and chat protocols. So was the intent perhaps to make it harder for leaks? It certainly didn't prevent Enron, or the financial collapse of 2009.

There is a growing inequality. Less information goes from the boardrooms to the outside world, while at the same time business collects more and more information about the public. The burden rests on whistle blowers, and the life of a whistle blower is not an easy one. Leaking sensitive information about malpractice in a business usually leads to firing, blacklisting, and poverty. It's still better than the life of

a person who leaks state secrets. Such individuals tend to get suicidal in the most creative ways.

Even darknets can't always survive determined leaks, as Chelsea née Bradley Manning and Edward Snowden showed. No security is perfect because it depends on people, and people make mistakes. Someone plugs an off-the-shelf laptop into a darknet, and suddenly it's trivial to copy gigabytes of documents to a USB drive. A maintenance engineer calls the head of operations warning that there's a problem with a router and they have to reset a password. However that "engineer" is a hacker and he gets the system password and access to every every server.

Given that no recording of a conversation is perfectly safe from being uncovered and leaked, how does the State handle the problem of whistle blowers? There are several strategies, as far as I can see. The most obvious and widely used is to attack any website that acts as a broker for leaks. WikiLeaks drew a massive amount of fire and fury for declaring its mission to be a broker for leaks, in 2006, leading to its founder Julian Assange infamously holed up in the Ecuadorian embassy in London, with Hollywood painting him in 2013 as a glory-seeking egomaniac. Threaten the powers that be, and you will pay.

While it can be tricky to arrest and disappear a public figure, it is trivial to launch a "distributed denial of service attack," or DDoS, on any troublesome website. One simply tells hundreds of thousands of slave PCs to request the main page of the website, say wikileaks.org, at the same time. The simultaneous volume of demand overwhelms the server so that real users can't access it. They give up, and the offending material stays unseen and unread. And where do you find a hundred thousand PCs willing to act as your go-to agents for an attack on wikileaks.org or whatever site is in the crosshairs today?

The answer comes from Redmond, in the form of Microsoft Windows, the most insecure and widely used operating system ever. It's

estimated that[78] 40-90% of Windows PCs are infected by some kind of rogue software — viruses, trojans, worms, and so on. The measured level is 42%, for *known* vulnerabilities. What about unknown holes in Windows, a so-called "zero-day attack"?

In June 2010, the Stuxnet worm[79] was found to be sabotaging Iran's nuclear program in a very sophisticated attack that looked for specific Siemens industrial control hardware, and interfered with it when it found it. Stuxnet is significant for several reasons, two of which are worth paying particular attention to. It was built by the NSA's hackers[80], and it used no less than four Windows zero-days.

Zero-days are very rare in theory. For a group of hackers to use four, in a single worm, hints that there are many more we know nothing about. So that 42% figure is low. It seems logical to assume that the NSA has worked to be able to access any Windows PC anywhere, at any time. I doubt that Microsoft directly created the vulnerabilities the NSA needs. More likely, Redmond has NSA teams discretely involved in the development of parts of the operating system, to "make it more secure," as the usual explanation goes. It's no shocker: the NSA publicly steers "secure" Linux and Android projects. So the figure of 90% seems more realistic. One would have to ask how the remaining 10% could possibly escape.

With more than a billion Windows PCs in use worldwide[81], that makes a lot of firepower. We've seen very large number of DDoS attacks on websites, even on entire countries[82].

A DDoS attack can be beaten off using the massive caching infrastructure of the Internet. People will simply copy interesting material,

78 http://ssd.eff.org/tech/malware

79 https://en.wikipedia.org/wiki/Stuxnet

80 http://www.usnews.com/news/articles/2012/06/08/nsa-built-stuxnet-but-real-trick-is-building-crew-of-hackers

81 http://www.businessinsider.com/right-now-there-are-125-billion-windows-pcs-worldwide-2011-12

82 https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

especially if the originating websites are being attacked. Trying to censor the Internet is like pouring petrol on a fire[83] to put it out.

A less visible and more effective plug is to cut financial support for the website. Big sites need hosting, and that costs money. WikiLeaks was the target of this in 2010, with US credit card processors cutting off all donations to the site. Despite not getting money from US contributors, WikiLeaks survived and got good press from being the victim of clearly abusive conduct by the US government and financial industry. So attacking a site will often just make it stronger. The very fact that authorities target a leaks site promotes its accuracy and importance. It is also technically hard to sustain.

In 2011, Bank of America hired three firms[84] to attack Wikileaks[85]. One of the firms, HBGary Federal, was hacked by Anonymous[86], and the plan was discovered. Emails and documents uncovered in the hack outline several proposed attacks on WikiLeaks:

> *Feed the fuel between the feuding groups. Disinformation. Create messages around actions of sabotage or discredit the opposing organizations. Submit fake documents and then call out the error.*
>
> *Create concern over the security of the infrastructure. Create exposure stories. If the process is believed not to be secure, they are done.*
>
> *Commit cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France, putting a team together to get access is more straightforward.*
>
> *Run a media campaign to push the radical and reckless nature*

83 https://en.wikipedia.org/wiki/Streisand_effect

84 http://wiki.echelon2.org/wiki/Team_Themis

85 http://wikileaks.org/

86 http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

of WikiLeaks activities. Sustain pressure. Does nothing for the fanatics, but creates concern and doubt among moderates.

Search for leaks. Use social media to profile and identify risky behavior of employees.

Once a leak is out and attacks on the website that released the information are shown to be useless, the next step is to attack the motives, sanity, and loyalty of the leaker. When there is a leak, the American press (when the leak concerns American secrets) focuses on the messenger and his motives, rather than the message. This isn't necessarily a conspiracy as much as how US media, and indeed much of US society, prefers style over substance.

The most significant trove of documents that WikiLeaks published came from Chelsea née Bradley Manning[87], who has been described in the media as mentally unstable, reckless, and naive[88]. Manning was placed into extreme solitary confinement on arrest, prosecuted in secret[89], and largely forgotten about until his conviction and sentencing for treason.

When someone leaks state secrets, as Manning and Snowden did, it is relatively easy to call out "traitor" and "national security" to trigger the tribalistic herd reflexes. Since those convenient attacks on 11 September 2001, we've been at perpetual war with an invisible enemy[90]. The state has a right to privacy, so the claim goes, and only a traitor would question that.

Perpetual war. It is straight out of George Orwell's 1984, and as a technique, it is working well. The War on Terror has given us a tame media that precisely reports the official line, no more or less, and investigates only superficially the inner corruption of the state.

87 https://en.wikipedia.org/wiki/Bradley_Manning

88 http://www.dw.de/the-trial-and-tribulations-of-bradley-manning/a-16839049

89 http://www.theguardian.com/commentisfree/2013/feb/22/bradley-manning-wikileaks-1000-days-detention

90 https://www.google.com/search?q=associated+forces

However, Orwell did not predict the Internet and how far it would devalue traditional media and propaganda.

I think the whistle blower is becoming the martyred saint of the Internet, the ultimate Original Poster, bringing us fresh and exciting content at enormous self-sacrifice. The way we view people such as Manning, Snowden, and Assange will be a litmus test of where we stand with respect to the future: for, or against.

Freedom to Share

All societies aggregate by remixing. We remix knowledge, and more broadly, we remix our culture. It's perhaps less formal a dance than the genetic remixing that occurs at conception, yet the process is broadly similar. Existing forms are brought together, remixed into new forms; these new forms are tested against real-world criteria and the successful forms are kept as sources for further remixing.

Let me make a basic observation about culture: it is the product of social collaboration. We make it through endless remixing of our own and others' work. There is no truly original culture, ever, any more than music, language, or ideas can be fully original. However, part of the creative drive depends on our individual ego, and the feeling that we're special, talented, and creative. So we lie to ourselves to overstate our own accomplishments and understate how much we borrowed from others. The lie can be very solid. A musician can hear a tune one day, and then sometime later, recreate the same tune with the total belief they are inventing something new.

This is one of those conflicts between the individual and society. As individuals, we believe in our originality and power to create and be different. As society we work together on a wide front, solving vast problems in countless little steps. This conflict can create a lot of drama in creative communities.

In the nineteenth century, a new class of enterprising lawyer-investor drew upon this myth to justify the creation of a raft of new laws: the so-called "intellectual property" laws. Modern patent

and copyright law, though very different in substance, share their common origin in this myth of the individual creator. This conflict was quite explicit in the debate around early British copyright law[91], with London booksellers arguing for infinite copyright, and the competing Scottish printing industry arguing for freedom to copy.

Modern patent law came into force in Europe in the mid-nineteenth century, with similar kinds of arguments. At this time, Germany, Switzerland, and the Netherlands had no patent system, while France and Britain did. Swiss pharmaceutics and Dutch electronics exist only because the absence of patent laws in those countries let them take others' processes[92] and improve on them.

At the start of this century, the US and Europe both had a nascent database industry (producing maps, phone books, and so on) In 2005, Europe made it illegal to copy commercial databases[93]. The US allowed such copying on the basis that the information in them was not copyrighted. Today, the US database industry is massive while Europe's is pretty much dead.

In technology, the free software sector, which effectively regulates a free-share zone, is massively larger, more successful, and more valuable to global industry than the proprietary software sector. Without free software, there would be no Facebook, Google, Web, Twitter, or Android. We would have the choice of Microsoft or Oracle. Yet today, the myth of the individual creator is still very strong. In the US, architects can use copyright law to stop people from photographing the design of their buildings, and copyright duration is now 70 years after death, which is effectively the infinite copyright that the London booksellers were demanding in the eighteenth century.

While copyright and patent law can be very profitable for the owners, those profits are always taken at a larger cost to society. Econom-

91 https://en.wikipedia.org/wiki/History_of_copyright_law#Early_British_copyright_law

92 http://www.guardian.co.uk/world/2002/mar/12/globalisation.comment

93 https://en.wikipedia.org/wiki/Database_Directive

ists have difficulty showing this, yet it's not for lack of data. Rather, working on this topic is a dangerous career move. Economists, like most ordinary people, have to feed their families and pay their mortgages. Very few have done extensive research into the real costs of the copyright and patent systems. The European Patent Office makes a habit of buying up economists who start to look at the economics of the patent system.

I'll explore patent and copyright in more detail in "Wealth of Nations". For now, I want to look at how they affect our freedom to share knowledge on line, why that matters, and what I think the outcome will be.

Thanks to the music and movie industries, "sharing" has been turned into an accusation and even a criminal offense in many countries. Among the hip and leading-edge, the "Would you steal a car?" propaganda clip is a joke. "Would you download a car to your 3D printer?" they ask, mocking the bookseller's claim that copying culture is a form of theft. Yet for the majority of people, the threat of disconnection, prison, or massive fines because someone shared a few songs by accident on the family WiFi is real and frightening. The outcome of this is that, while people are confident in sharing photos of their cats and kids, they're less keen on stepping outside the walled gardens that Facebook and its ilk provide.

It is very convenient for the establishment that the Internet is divided into "good" and "evil," where "good" encompasses people who take no risks and do nothing unusual, and "evil" consists of the criminal hackers, pirates, child pornographers, and terrorists. Once you decide to draw such a line, it becomes a snare around the neck of the quiet majority.

Why does this matter? Who cares if the bulk of Internet users never venture beyond the safety of the manicured gardens of their social networks? After all, the average person has an IQ of 100, thinks Adam Sandler is funny, and types with one finger. It matters because people are only as stupid as their environments. That average person is the

descendant of an infinite line of survivors, each meaner and more determined than their peers. Inside every calm, ordinary person sits a little implacable demon, able to come to life, grow and take charge if the situation demands it.

Bread and circuses. The criminals inside the ring, fighting the wild animals, and the spectators outside, passively watching. That was the way the establishment hoped the Internet would develop. Except that the crowd jumped the barriers and joined the fracas in the ring.

In 2008, the Church of Scientology tried to use copyright law to censor the video interview of a prominent Scientologist, Tom Cruise. YouTube complied. Other websites refused, and the loose communities calling themselves "Anonymous" decided this censorship was a casus belli. It wasn't the first time Scientology hit the Internet.

In 1995, they sued a Dutch writer and Internet service providers for the leak of secret "church teachings," losing after ten long years in the courts. However, while the previous fight took place in the courtroom where Scientology's money could work effectively, this new fight took place on the Internet, where, curiously, all of Scientology's money was worthless. This raises a side question, which I'll return to somewhat later, of exactly what currencies operate in this strange world.

Wikipedia tells the story[94] thus, "Project Chanology was formulated by users of the English-speaking imageboards 711chan.org and 4chan, the associated partyvan.info wiki, and several Internet Relay Chat channels, all part of a group collectively known as Anonymous, on January 16, 2008 after the Church of Scientology issued a copyright violation claim against YouTube for hosting material from the Cruise video."

Before this, Anonymous was best known for ordering lots of pizzas for people they didn't like. Chanology was their first real fight, and out of that conflict emerged something surprising in its scale, and

94 https://en.wikipedia.org/wiki/Project_Chanology

breathtaking in ambition. Up until this point, Scientology was a very powerful international organization. They had subverted the US Internal Revenue Service (IRS) and paid no taxes. They were able to make people disappear without consequence. They had friends in high places, and their lawyers scared the most defiant of websites into silence.

What Chanology became was the focal point for thousands upon thousands of people who hated Scientology for strong personal reasons. Either they were ex-members, or they had lost family or friends to the cult. These were ordinary people, not youthful hackers with nothing to lose. They went to Scientology offices and protested. They went to on-line forums and talked.

Anonymous told Scientology[95], they had "decided that your organization should be destroyed." And this is pretty much what has happened. They tore through the blanket of acquiescence, as Scientology's feared lawyers found themselves unable to stop the leaks and discussions. They spread those secret "church teachings" far and wide, and mocked them for being poorly-written sci-fi trash. They exposed Scientology's most precious internal secrets — documents, money, names, and dates. The aura of success that people like Tom Cruise had cultivated through their membership of Scientology became a badge of pity, even in the mainstream press.

Scientology was just the first real fight for Anonymous, which has become the armed wing of the Internet, despite not even being an organization at all. They have started to take on the State itself.

Project Chanology showed what a large, diverse, angry, yet highly sane crowd could do, when they ignored the lawyers and the copyright claims, and focused on a real political objective, and a Bad Guy. I recall an elderly woman in France telling me there was an on-line vote on whether Scientology should be banned. Apparently the Scientologists had been voting *en-masse* for a "Non," which was at 60%. She was furious, in her firm, grandmotherly way. So I set up a few cloud

95 http://www.youtube.com/watch?v=JCbKv9yiLiQ

servers and we downloaded a voting script some anon had made. After a few hours, the Oui vote was at 90%.

It is sometimes harder to convince the crowd to jump over the barrier and get involved. There are real risks and the benefits can seem faint or unpredictable. Though the Piratebay torrent site tried to provoke a fight over copyright, most people are content to use Spotify and Netflix. Apparent civil obedience, breaking the rules when we can get away with it, is still easier for most of us than open confrontation, anonymous or not.

Summing Up

In this chapter, we looked at freedom as "being able to do interesting things with other people," and we looked at how freedom is essential to a healthy, wealthy society. We looked at how a regressive establishment tries to control digital society by reducing its freedom, and how digital society fights back. I hope I've given you tools for better understanding what is going on with WikiLeaks, Anonymous, and so on. In the next chapter, we'll look at privacy. More accurately, we will try to understand its disappearance.

Chapter 5. Eyes of the Spider

If the Culture ran on light, thought the Empire, then it would destroy light.

Privacy isn't totally dead yet, although we are very close. It's happened rapidly, over the last fifteen years or so, as the political and technical barriers that stop others from monitoring us have fallen away.

Every credit card purchase we make is recorded. Where, when, what, how much. So is everything we buy at the supermarket using our loyalty card. So is every trip we make by air, or by train and bus, if we use an electronic card to travel, or to pay. So are details of every film we watch or rent, if plastic comes into the picture somewhere. Every book we check out from a library, or buy on line, is recorded and stored in a database somewhere.

Every website and page we visit, when, for how long, and where we came from. What emails we send, to whom, and what we say. Every search we make, every post and comment on any forum anywhere. Who we call or chat with, when, and what we say.

Our own mobile phones track us like pigeon collars: where we are, to the closest 50 yards, across almost the entire habitable globe. Every call we make, who we call, and what we say. Our fixed phone lines were already bugged decades ago. When we're on foot or in our cars, where we go, whom we meet, how long we stay: it's tracked by cameras posted in public and corporate spaces, and recorded, and stored.

The list goes on like science fiction. The spy state is well leaked and documented, though we can assume there are large secret surveillance systems, like those of the FBI that were discovered only by long and determined work to open classified documents. And these are not just simple databases. They are parts of a puzzle — your life — that the

state and big business are carefully putting together, one piece at a time.

This is the story I'll tell in this chapter: the death of privacy. I'll try to explain how it happened, how it affects us and why that matters, and what digital society can do about it.

Enter the Spider

There is an alphabet soup of agencies that spy on us. Today the NSA makes the news, tomorrow the headlines may be about the British General Communications Headquarters (GCHQ), the US Federal Bureau of Investigation (FBI), Office of Naval Intelligence (ONI), the Department of Homeland Security (DHS), or Israel's Mossad. It would be naive to assume there is one single agency that has all the software taps and hard disks. Rather, it's a network of agencies and programs and databases that reaches around the globe, penetrating and corrupting business and politics.

Furthermore, it seems implausible that this network operates independently, outside of any political structure. Where there is power and money, there are always political structures. The political structure behind the spy state is simply not the one we vote on, or exert any real control over, as governed.

Silvia Swinden, a writer on human rights, nonviolence, and humanism, coined the term "Para-state"[96] to describe the "rich bankers and industrialists, royalty, corporations and most powerful politicians of the world" who meet yearly as the Bilderberg group.

And indeed, we see the formation of a parallel global state, with its own citizens, its own laws and courts, its private security forces, its physical and social isolation from the rest of humanity. It's an old storyline in the futuristic dystopia, from Fritz Lang's 1927 movie Metropolis and The Time Machine from H.G. Wells, through to modern tales such as the 2013 movie Elysium. In that movie the wealthy liter-

96 http://www.pressenza.com/2013/06/the-economic-para-state-in-its-yearly-show-of-strength-bilderberg-comes-to-watford-uk/

ally live off-Earth on an orbiting mini-planet. In reality of course, there is only one Earth, we are all stuck on it, together. Humanity will survive as one species, or die as one species.

Yet despite the obvious face-in-palm insanity of global apartheid, it seems to be what those unnamed political structures are striving for. And here, as a writer, I face a problem. One cannot examine things without names, nor can one resist forces without names. I cannot say "NSA" when I mean the powers behind it. Nor can I say "Empire," for that's a parable. Nor will I use any of the labels that the "New World Order" conspiracists enjoy, loaded as they are with fear, hate, and anthropomorphism. The only one I like is "Lizard People," except some readers would take it seriously.

So Silvia Swinden's "Para-state" is the term I will use, to describe the old power structures that digital society is laying bare, and confronting, and will eventually overcome. Whereas the State derives its power from the governed, the Para-state feeds off the State and treats the governed as the enemy.

As for the NSA and its fellow alphabet agencies, and including without prejudice all businesses and criminals involved in spying on us, I'm going to use the term "Spider," which is what early Internet geeks called the computer programs that "crawled the world wide web." It wasn't a great pun then either. However, I rather like the notion of a massive thing with eight legs, eight eyes, sharp venomous teeth, and no brain to speak of, implacably stalking us as we struggle with our pathetic little lives.

The Spider is nothing to laugh at, however. It reaches around the world, into every communications network and technology industry, into every country that has not raised a strong firewall against it. It has global reach and immense budgets. It employs armies of private contractors[97], both civilian, and military — mercenaries who operate outside national laws. And the Spider does one job: protect the Para-state

97 http://www.policymic.com/articles/48845/booz-allen-hamilton-70-of-the-u-s-intelligence-budget-goes-to-private-contractors

from threats. It exists outside conventional political reality, disconnected from the democratic process, making up its own definitions of constitutionality and legality, as it goes along.

The Dollar Yoltabyte

Is it paranoia to assume every phone call is recorded?

It seems clear the political will to spy on us is there, and has been for some time. That, by itself, is extraordinary, given the history of the last century. The "free" West positioned itself opposite the spy states of the Soviet Empire. In Europe, we had solid laws limiting the collection of personal data. The US had solid laws protecting privacy. These seem to be washed away as if they'd never existed. The story of how that happened is worth exploring, and I'll do that. First, I want to crunch some numbers.

Since politics said "yes" to the spies years ago, the limiting factor has been technical feasibility, and subsequent cost. There's a limit to how much a government can spend on surveillance before it shows on the budget. Let's estimate the cost to store and process the data produced by the domestic US market at various points in time.

How much data are we talking about?

Over time our use of communications has shifted significantly. In 2000, it was mainly mobile phone calls. In 2013, it's far fewer phone calls, and a lot more chats and text messages. We also produce and consume a lot more content in the form of photos, videos, documents, and so on. There are also more of us on line.

The vast majority of Internet traffic is, however, irrelevant to the spies, or already stored by cloud services. For example when you watch a YouTube video, does the Spider need to store the video stream? It only needs the YouTube URL, and metadata such as when you watched, when you pressed play and pause, what site you came from, and so on. Similarly for those photos you upload to Flickr. All the Spider needs is a guarantee from Yahoo! that it will store them forever.

The actual amount of useful information one person can generate is fixed. Even if we type or click faster, its not going to grow exponentially. So we can assume the data the Spider must collect is only growing incrementally over time, and thus presents a slow-moving target. I will call this the "target data set" (TDS).

To calculate the TDS size, I'll take the US domestic market with its population of about 300 million, and I'll assume a modest average amount of surveillance:

- 15 minutes of video surveillance (closed-circuit television, or CCTV): about 100MB per day.
- One hour of audio surveillance (phone calls): about 50MB per day (half of 100MB).
- Four hours of web surveillance (clicking and typing): about 5MB per day.
- 24 hours of location data (mobile phone and license plate tracking): about 1MB per day.
- Other surveillance (credit cards, shopping, etc.): about 1MB per day.

That's a total of 157MB per person per day. Multiplied by 300 million, and 365 days, that gives us 17.2 exabytes (1.72E19 bytes) per year. Rounding up, we get 20EB as our TDS size. If you enjoy useless imagery, that's a stack of 1TB hard drives 135 miles high.

It's probable that the Spider can automatically transcribe phone calls. It seems an obvious research area, essential for automated scanning of conversations. Such text would be much smaller than the audio data. However the Spider would still store the original audio, just to be safe. So this doesn't affect our calculations.

Now, the cost of storing this 20EB target data set. Over the last 30 years the cost gravity of hard disks has been 14 months, giving a 90% price fall every four years. That high stack of drives collapses to one-tenth its size every four years. Here is how much you can store for one US dollar, from 1990 and into the next fifty years:

1990	100KB
1994	1MB
1998	10MB
2002	100MB
2006	1GB
2010	10GB
2014	100GB
2018	1TB
2030	1PB
2042	1EB
2054	1ZB
2066	1YB

For comparison, the total bytes of DNA in a human body (treating the human body like a hard disk, and ignoring that our cells have almost the same DNA) is about 150ZB (100 trillion cells at about 1.5GB per cell), and there are about 21 yolta atoms in a gram of silicon. I think the dollar yoltabyte will happen right on schedule fifty-some years from now. Side note: the prefix "yolta" was only coined in 1991.

Hard disks are only the raw cost. Let's assume we store all data in two different data centers, to guard against disasters. In each location we add backup disks to guard against disk failures. We need industrial-strength disk storage racks, power supplies, cooling, and maintenance. We need at least 15% for bribes and consultancy fees back to the congressmen who voted us the budgets. We get a volume discount. Let's assume all that makes a cost factor of four.

So here's the real cost over time of storing the TDS from 1990 through to 2050, falling about 350 times every 10 years:

1990	$687.7T

1994	$68.8T
1998	$6.9T
2000	$2.2T
2004	$217.5B
2006	$68.8B
2008	$21.7B
2010	$6.9B
2012	$2.2B
2014	$687.7M
2016	$217.5M
2018	$68.8M
2020	$21.7M
2024	$2.2M
2030	$68,766
2040	$217.46
2050	$0.69

Clearly as late as 2006, it was only possible to store data only on a fraction of the population, the so-called "Persons of Interest." These make a nice data set for several reasons. First, no politician who cares about elections is going to refuse a request to spy on a potential terrorist. Second, these people produce data that can be cross-checked with real-life events such as political protests or bombings. Third, it's a data set that can be expanded organically to cover everyone.

That expansion has happened. The TDS has grown (by the Spider's own account) from persons of interest, to anyone they talk to, which is one degree of separation, or one hop. Then, anyone *those people talk to*, or two hops. And today, three hops. This easily covers the whole domestic population. "Talking to" someone could simply mean visiting the same website.

Though these figures are just estimates, they show the overall trend. There's a moment, perhaps 2012 or 2014, where a full TDS becomes affordable. There's a moment, in 15 to 20 years, where the cost becomes so low that there will be dozens or hundreds of organizations

doing this. Any attempt to stop surveillance by budget control becomes impossible. By 2030, the cost of global TDS, covering 10bn people, will be just a few millions. By 2050, it is a child's weekend project.

The Drying Lake

Because of cost gravity and politics, privacy is dying in the twenty-first century like a lake in a drying desert. This is a one-way and unstoppable process, caused simply by the asymmetric nature of information. It is much cheaper to spy on someone than it is to prevent people from spying on you. As Cost Gravity pushes down the cost of cameras, networks, hard disks, and CPUs, the cost of maintaining privacy grows higher and higher. In the end it comes down just to politeness and ethics and restraint, things we can expect of other individuals, just not of businesses, nor of governments.

The death of privacy has costs, and benefits, depending on the situation. Our secrets are our property, and losing them devalues us. Those same secrets may benefit many more people, when they become public knowledge. When the cost of secrets held by one person or group outweighs the benefits to society, then it's right that those secrets be leaked. Health research based on population-wide data can help, for instance, to pinpoint causes of illness and disease.

Yet personal privacy remains a core requirement for individuality. Losing our privacy makes us weaker, easier to manipulate, and easier to control. Vitally, we lose our taste for critical analysis, and we stop demanding information. The invasion of privacy is not just about stopping terrorists, or making more money off us. It is a basic mind-control technique. Every cult starts by isolating people from wider reality, whilst forcing them to live in something like a commune.

I think we've seen the deliberate stripping of privacy used with wide effect. The passivity of the American public is famous, and confusing. After all, these are the descendants of people who crossed

oceans to fight for a better life. Americans can get very angry about little things. Yet, when it comes to the shenanigans of their leaders, the majority response seems to be "Yeah, well, what you gonna do?"

Bad Things Come in Threes

There are, overall, three columns fighting the War on Privacy against the digital citizenry. They work together often, overlap quite significantly, share techniques and knowledge, and presumably they answer to the same range of pay masters in many cases.

The first column works for business, particularly the web industry, which tracks us obsessively. The range of techniques used to spy on us would be breathtaking if we were not all so cynical. Every page is filled with little tracking devices. Every click sends back traces to databases, and profiles are fattened up, cross-indexed with data from the real world and other sources, used for targeted advertising, price manipulation, and market research. Data is bought and sold like pigs in a market, breaking every possible regulation on personal data protection. There is no real escape, and we accept that the "free" Internet has this as one of its costs.

The second column work for themselves. They bug our PCs with viruses, trojan horses, worms, and spyware. They watch what we type, steal our credit card information and bank details, passwords, and emails. They control the best part of a billion PCs worldwide, largely thanks to Microsoft's inability to make Windows secure.

And the third column works for the state. We're not talking about one country, rather, of coalitions of varying degrees of integration. Centrally, the Anglophone axis[98]: Canada, US, UK, and Australia. Even New Zealand goes along for the show. Secondarily, NATO around that: Germany, Italy, Turkey, France. Third, the silent partners: Israel, Egypt, Saudi Arabia, Pakistan, Sweden, Japan, South Korea. And then the Independents: China, Russia, India, and Brazil,

98 https://en.wikipedia.org/wiki/UKUSA_Agreement

building their own networks and sharing very little, if anything, with the west.

It's the third column that is the most dangerous to digital society, because their prime goal is the control of political discourse. They don't want to make money from us, or use our PCs to send spam. They want to make sure we don't build a revolution.

The third column's strength, at least in the US, comes from two things. First, unlimited secret budgets, enabled by the "War on Terror," and the signing of the PATRIOT Act in October 2001. Second, the highly centralized nature of today's web. A handful of phone companies control Internet access for most people, and a handful of websites account for most Internet traffic. The capturing of the airwaves is an old sport. What's shifted is the sheer volume and focus. It's the mass digitization of social activity, and its concentration, that has created fertile ground for the greatest spy regime of all time.

The Listeners

In 2013, Edward Snowden focused the public's attention on the scale and audacity of the global surveillance state, mainly the American parts, and the roles played by the UK and France. The goal of this surveillance state was, and presumably still is, to *know everything about everyone, all the time*.

However, the growth of the global surveillance state wasn't really news. We've been hearing reports of this for some time. The grandfather of spy networks, ECHELON[99], started intercepting international phone traffic almost as soon as it was technically feasible, in the 1950's and 1960's.

As Kevin Drum wrote in Mother Jones[100] about the NSA tracking credit card use:

This is sure starting to sound a lot like our old friend, Total In-

99 https://en.wikipedia.org/wiki/ECHELON

100 http://www.motherjones.com/kevin-drum/2013/06/wsj-nsa-program-also-tracking-credit-card-transactions

> *formation Awareness. You remember TIA, don't you? It was the Bush-era program designed to tap into commercial and government databases across the country and hoover up credit card statements, medical records, travel plans, phone bills, grocery receipts, and anything else that sounded interesting. Congress killed it in 2003, but forgot to salt the earth behind it. TIA didn't die — it metastasized.*

In August 2007, Wired magazine reported that[101] "The FBI has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device, according to nearly a thousand pages of restricted documents newly released under the Freedom of Information Act."

That state agencies have modern technology is normal and expected. The surprise is the ease with which traditional political barriers to intrusive surveillance have been set aside. It used to be that a wiretap required a physical action by a phone company, acting on a court order. Now, wiretapping functionality is built-in to phone equipment and networks by law and accessed through the click of a mouse. As Wired explains:

> *...the surveillance systems let FBI agents play back recordings even as they are being captured (like TiVo), create master wiretap files, send digital recordings to translators, track the rough location of targets in real time using cell-tower information, and even stream intercepts outward to mobile surveillance vans.*

101 http://www.wired.com/politics/security/news/2007/08/wiretap

It sounds nice: a powerful set of tools that give agents everything they need. There are two problems. First, the systems assume we can blindly trust the intelligence agencies not to click that mouse until the court has issued an order. This seems extraordinarily naive. The second problem is that powerful tools are regularly misused, either by corrupted insiders or well-informed outsiders. As Wired notes in the same article:

> *More than 100 government officials in Greece learned in 2005 that their cell phones had been bugged, after an unknown hacker exploited CALEA-like functionality in wireless-carrier Vodafone's network. The infiltrator used the switches' wiretap-management software to send copies of officials' phone calls and text messages to other phones, while simultaneously hiding the taps from auditing software.*

CALEA was the FBI's wiretap system at the time. That "unknown hacker" turned out to be working out of the US Embassy, in cooperation with Vodafone. The network planning manager in Vodafone had one of those mysterious suicides[102]. Snowden revealed, somewhat later, that the NSA has been bugging officials across Europe.

The NSA, formally responsible for spying on foreigners, runs what is perhaps the world's largest hard disk array[103], in Utah. Responding to allegations that this facility was being used to collect data on US citizens, the NSA denied they were "unlawfully listening in on, or reading emails of, US citizens."

That critical "lawfulness" of the NSA's surveillance is governed by the Foreign Intelligence Surveillance Act (FISA) and decided by a secret court, FISC[104]. FISC judges are appointed without oversight, and their rulings are made in the dark and locked up forever. Until, that is, someone leaks them.

---

102 https://en.wikipedia.org/wiki/Kostas_Tsalikidis

103 https://en.wikipedia.org/wiki/Utah_Data_Center

104 https://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court

One of Snowden's juicier leaks was a top secret court order issued by FISA that required Verizon, a US phone company, to provide a live feed of phone calls — including those for domestic calls — to the NSA. In 2012, the government presented 1,856 applications to the FISC, which approved 100% of them[105].

Let's skip around the obvious and massive loopholes such as "we only spy on foreigners." Presumably Americans count as "foreigners" to the UK's GCHQ[106], which captures every single Internet packet it sees, and merrily exchanges data with the NSA. And presumably the NSA doesn't speak for the other alphabet agencies when it says "we".

More interestingly, there are claims[107] that the NSA's surveillance program started some time *before* September 11th. In February 2001, a full seven months before the War on Terror officially started, the NSA asked four US phone companies to turn over call records to an NSA database, offering secret contracts as an incentive. The request was illegal and a violation of federal privacy laws. AT&T, Verizon, and BellSouth turned over their records nonetheless. Just one firm, Qwest, stated publicly that they would not take part until served with a valid court order.

The court order never came. Qwest didn't get the NSA contracts or money either, and by 2002, overwhelmed by debt, was being sold off in chunks to private equity firms. Its ex-CEO, Joseph Nacchio, was charged with fraud, convicted, and went to prison in 2009. Its Chief Operating Officer Afshin Mohebbi was cleared of all fraud charges in 2011.

The Electronic Frontier Foundation (EFF) wrote in December 2007 that, "after months of pressure from the Bush Administration, the full Senate is poised to grant retroactive immunity to these compan-

105 http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests

106 http://www.spiegel.de/international/world/snowden-reveals-how-gchq-in-britain-soaks-up-mass-internet-data-a-909852.html

107 http://www.wired.com/threatlevel/2007/10/nsa-asked-for-p/

ies, which would effectively ensure that the full extent of their complicity will never be known." The collaborating phone companies were given retroactive immunity in July 2008. Nacchio was released in October 2013, to somewhat of a hero's welcome, given Snowden's revelations.

As a side note, all anti-trust actions against these mobile phone companies stopped in 2000, and the US government allowed them to merge and reform the phone cartel[108] that the regulators had broken up in 1984. In 2006, AT&T merged with Bellsouth, leaving it and Verizon with two-thirds of the 300 million mobile phone subscribers in the US.

For me, the really interesting parts of the Qwest story are how the spying on Americans started before the War on Terror, not after, and the level of bribery and blackmail that governments seem willing to focus on industry to get their collaboration.

Perhaps Qwest was doomed due to debt accumulated after the dot-com crash, and its CEO was corrupt anyhow. It's hard to imagine a corrupt man refusing bribes, and taking such a principled stand. The simpler explanation is: you work with us, and we'll take care of the legalities afterwards. You'll get market share and secret cash. And if you resist, or if you talk about this deal, your company *will* die, and you *will* go to prison. When you hear the CEOs and spokespeople of thriving corporations denying their level of cooperation with the NSA, you need to question their freedom to tell the truth. When a firm receives a National Security Letter, it is obliged by law to deny that fact.

The tragic irony is that it's the nicer business executives, the 96% or so who are not psychopaths, who buckle under such threats. It takes a peculiarly tough disregard for authority and their sanctions, one close to a mental disorder, to stand up and fight bribery and corruption when all those around you are losing their heads, as it were.

---

108 http://technologizer.com/2011/03/20/att-buys-t-mobile/

Analysts Retentive

In the hot summer of 2013, following the Snowden leaks, European governments angrily denounced the American surveillance state. Their flamboyant shock and horror reminds me of a careless driver, who after causing five accidents, explodes in rage because someone cuts in before him at the intersection.

My first encounter with the global surveillance state was in December 2005, when the European Union passed the Data Retention Directive[109], or DRD. At the time, we in the FFII and some allies lobbied against this law, and we were pretty much alone. Political parties left and right united to push the law through with little debate. National governments supported it, with a few exceptions. At the time, we reported:

> *The so-called "Big Brother" directive, highly controversial at least among those even aware of its existence, requires all Internet and telecommunications service providers to log all traffic metadata (who called who, who visited what sites) in Europe for 6 to 24 months and turn the data over to police forces, secret services, and other organisations, as decided by national governments. The law was drafted and passed in three months, an extraordinarily rapid process, and was heavily influenced by earlier UK legislation that failed to pass in Britain.*

The DRD was written in a hurry, and sold to a compliant European parliament as necessary to Save the Children from Organized Criminals and Terrorists. It was one of several anti-Internet laws passed in that decade, at high speed, and in silence. The Intellectual Property Rights Enforcement Directives (IPRED) criminalized copyright and patent violations, which were traditionally civil disputes. The Telecoms Directive regulated the telecoms market (and did noth-

109 http://en.wikinews.org/wiki/Data_Retention_Directive_passed_by_EU_Parliament

ing to stop the roaming mobile broadband banditry across Europe, the one issue regulators should have tackled).

The DRD had two main features. First, it cracked down on anonymous access to the Internet and telephone systems. No more access to Internet cafés without identification. No more mobile phone subscriptions without papers. If this hurt undocumented immigrants, so much the better. Second, it required Internet service providers (ISPs) and phone companies to collect metadata on all communications (emails, phone calls), store this for several years, and make this available to governments.

The process by which the DRD was passed was quite the lesson in how to sell impossible laws to the public. Let's remember that the US was pushing for exactly the same kind of surveillance. So this was probably the generally agreed upon policy of the governments of the West. However, it was a difficult sale given Europe's staunch history of data protection, in other words, laws to limit how much data could be held on individuals. In 2004, the Westminster parliament roundly rejected a proposal from the Blair government to collect and store metadata on phone calls and emails. I can imagine their televised outrage at the idea.

The next day (metaphorically speaking, for I'm sure there was a pause for sandwiches and wine), the UK government was in Brussels. They laid their proposal before the European Commission. We don't know how the discussions went, though they cannot have been difficult. The Commission wrapped up the British proposal as a Directive, without the usual public consultations, and laid it before the Brussels Parliament. It basically told them, "If you're against terrorists, and cybercriminals, and pedophiles, you will vote for this," and the European Parliament did just that, overwhelmingly.

The UK government then took the new European legislation back to London. They presented it to the Parliament in Westminster, and said, to paraphrase, "Sorry, chaps, it seems those damnable Eurocrats have done it again. We've no choice except to ratify this one." Just be-

fore tea and more sandwiches, they decided, with televised regret, to vote the DRD into British law. There was no real alternative, was there?

In Germany, the DRD was ruled unconstitutional and was not implemented. Other countries embraced the legislation. Here's how Wikipedia describes Italy's enthusiastic implementation[110]:

> *Internet cafés and public telephone shops with at least three terminals must seek a license permit within 30 days from the Ministry of Home Affairs. They must also store traffic data for a period which may be determined later by administrative decree. WiFi hotspots and locations that do not store traffic data have to secure ID information from users before allowing them to log on. For example, users may be required to enter a number from an ID card or driving license. It is not clear how this information is validated. Mobile telephony users must identify themselves before service activation, or before a SIM may be obtained. Resellers of mobile subscriptions or prepaid cards must verify the identity of purchasers and retain a photocopy of identity cards.*

Britain was then, and still is, creating what must be the most dense surveillance state in the known universe. In London there are approximately 2,031 cameras per head of population. OK, that figure is a joke. The real figure is somewhere between "a lot" and "you *cannot* be serious"). So the DRD, with its shifting of the burden to private industry and the bulldozing of data protection, came at an opportune time.

Much of what the DRD mandated wasn't even possible then. ISPs scratched their heads, wondering where they were going to find so many hard disks. Of course, technology caught up, and by the time of the First Revelations of St. Snowden, the NSA's little brother in Bri-

110 https://en.wikipedia.org/wiki/Telecommunications_data_retention#European_Union

tain, GCHQ, was storing three days of all Internet traffic crossing the UK. Using my previous TDS calculations, for 60 million people, that's 30 petabytes, or 30,000 terabyte hard disks. That's less than $1 million in 2013, which is pocket change.

The Whale Shark's Maw

It still sounds like a lot of data to process in real-time, like in the movies. I'm sure real-time tracking is part of any modern surveillance system, limited to a tiny number of high-interest targets, such as politicians, lawyers, judges, journalists, activists, and so on. It needs a live person at the controls.

The bulk of the work has to be automatic processing of the raw data, at multiple levels. There is a science to this, and it explains why the security apparatus obsessively expands its data sets, and why it probably keeps them forever, no matter what the law says. I'll explain one possible approach. This is not a factual account; it's just one plausible strategy.

The raw streams are published out to thousands of different "detectors." A detector requests specific slices of data and searches for particular keywords or patterns. These patterns could include when a person uses a specific keyword in a phone call, or visits some website, or makes a particular kind of purchase. Each person's data is in effect a separate stream, so the detectors can be run on any number of compute nodes. The raw data is recorded so that different detectors can be run over and over on real historical data.

The detectors produce matching "events." These events are indexed in databases, and a series of "trawlers" scan these, looking for correlations between multiple individuals. Perhaps two persons of interest were in the same location at the same time. Maybe one man tagged as "homosexual" met another man in a hotel for an hour, the day after exchanging emails.

The trawlers produce "hits." Each hit provides a potentially interesting fact. Most hits will be false positives, which are too expensive to

filter out by hand. So the next step is "filters" that remove false positives using different heuristics. What's left is a high-quality (at least in theory) stream of positive hits that the expensive and slow human analysts can examine.

To do this work on realistic data sets requires a lot of "pre-computation." I'll give one example. If 10,000 compute nodes are working on the raw data, a naive algorithm would have to make 10,000 comparisons against each incoming piece of data. That would not be fast. To be fast, we must first pre-compute an index that turns any given keyword into a set of compute nodes. We can then hash any piece of data into a set of keywords in constant time, and turn that set of keywords into a list of compute nodes also in constant time. It makes the difference between processing 1,000 pieces of data per second and processing 10 million per second.

This excludes real-time "what if" scenarios. These are possible on small data sets, such as the stream for a single individual. It's not possible on the real raw data. Instead, the analysts improve their detectors, trawlers, and filters over time by seeing where they don't work perfectly, and improving them there.

So for example, if the FBI missed the Boston Bombers of 2013 (which they apparently did), they'll go back to the data set of those individuals — back 2, 5, or 10 years — and try different algorithms. Eventually, they'll develop better ones that could have given positive hits on these young men. They can then replay those algorithms on other data to check that they make sense and don't produce new false positives. Once the new detectors, trawlers, and filters are working, they are plugged back into the production systems.

The tools don't need to be perfect today. For such data mining to work, one need only collect enough data and hold it forever. Any new detector or algorithm must be retested against historical data and historical events to make sure it is better than previous ones.

From the perspective of the ones building these systems, storing everything forever is a logical answer to a real problem. There are pri-

vacy laws, which are for other people. No spy was ever convicted for breaking a law on privacy.

This obsessive tracking of our private lives is of course entirely asymmetrical, and wasteful. It makes us all criminals, all the time. Society cannot be divided into those with nothing to hide and the terrorists. This collected data can be leaked, used to blackmail politicians, stolen, and sold. It's certain that this collection of our private lives as the exclusive privilege of gray men who work for the rich and powerful is not a good thing.

Having said that, the cost of tracking everything about us is falling by 50% every two years or less. Sooner or later the monopoly of power that the alphabet agencies enjoy in this domain will be gone. This is, I think, the real outcome: cost gravity will take those emperors' toys and make them commoners' tools.

In the meantime, exposure of the Spider's and Para-state's own secrets provides something of a balance. Those most ready to attack others are usually also those with the most to hide. I can't wait until the first leak of the full files for every single Congressman.

Skynet, I Presume?

One of the groups processing what the Spider sees is the Special Operations Division (SOD) of the DEA. In August 2013, Reuters reported that[111], "*A secretive US Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans.*"

The SOD unit, numbering several hundred people, shares information with the FBI, NSA, CIA, IRS, DHS, and half a dozen more agencies. The unit was created in 1994 to fight Latin American drug cartels.

111 http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

It is true that the Mexican drug cartels are undoubtedly vicious[112] and if they lived on my doorstep, I'd probably bless any agency who asked with the powers it asked for to fight them.

There are strong arguments that drug prohibition created these cartels in the first place, and law enforcement budgets that depend on them in the second. Every police force eventually forms a symbiotic, and profitable, relationship with the criminals it is meant to catch. Let's set that aside for now, though.

I see two red flags in the SOD's work. The first is the sharing of information with other agencies. This may sound innocuous, even sensible. However, what it means is that those 12 agencies are building an integrated spy network. "Sharing" is a euphemism for "standardizing data formats and real-time interconnectivity." Before, we have a dozen or more autonomous and disconnected agencies. After, we have the Spider. This of course makes sense for enforcement. It is, however, an extraordinarily dangerous tool. As we've seen, law enforcement is not neutral.

Not least, as the Guardian wrote in 2012[113], the Spider takes orders from the banking industry. This is the same industry that in 2009 received $352 billion[114] from those drug cartels which excused the creation of the Special Operations Division to start with. This influx of cash saved many banks, according to Antonio Maria Costa, head of the UN Office on Drugs and Crime.

The second red flag is the use of "parallel construction" to fake the evidence trail. Ostensibly, the goal is to protect informants and sources. However, Reuters' report shows it being used instead to conceal links with the NSA, in other words to hide the existence of the Spider. Suddenly, the Spider is targeting US citizens. Reuters adds

112 https://en.wikipedia.org/wiki/Miguel_Trevi%C3%B1o_Morales

113 http://www.guardian.co.uk/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy

114 http://www.theguardian.com/global/2009/dec/13/drug-money-banks-saved-un-cfief-claims

that "the SOD's mandate has expanded to include narco-terrorism, organized crime, and gangs."

The slippery slope goes one way. From drug dealers to growers, and small time dealers. From gangs to anyone who has been in prison or lives in a poor neighborhood. From terrorists to political activists and campaigners, and eventually anyone who threatens the establishment.

Society has largely tolerated wire-tapping because the security services only targeted "foreign terror threats." Parallel construction (aka, "intelligence washing") tries to maintain that pretense. However, as "anti-terrorist" intelligence is used more and more in straight-forward criminal cases, we'll see the term "domestic terrorism" expand. Eventually the pretense will collapse and it will be clear that the security services are focused on political dissidence above all.

The Bogeyman Cometh

As we FFII volunteers worked in Brussels, without success, against the Data Retention Directive in 2005, I wondered what the real back story was. The argument that "this is against terrorists/cybercriminals/pedophiles" seemed — and still seem — fatuous. The sheer cost, in financial terms, and in privacy terms, seemed disproportionate.

The fact that the UK was the driving force behind the DRD seems significant. Why, I asked myself, was the UK government so obsessed with putting every one of their citizens under complete and secret surveillance with no judicial or legislative oversight? Technically, "domestic spying" is banned by any country with a sane constitution. We've had enough experience of what happens when the State allows this to happen. At best, it's a stifling blanket that turns the country into a poor, tired, cardboard box of a place. At the worst, it leads to the collapse of reason, and self-destruction.

The question no one seems to be asking is, "Why?" Why would the UK government want to spy on their citizens and push the whole EU to follow? There was, after all, no real political dissent, no dramatic challenge to established authority, no risk to the political elite that

they would lose their grip on power. The unspoken deal was, you continue to give us cool gadgets and digital toasters and the Internet. In return, we'll ignore your thievery, whoring, and corruption of the peaceful society for which our parents and grandparents fought.

It is true that the EU Parliament passed the DRD in February 2006, six months after the London bombings. However in June of 2005, one month *before* the London bombings, the European Parliament had already rejected the draft proposal[115]. It was finally passed only by force; the European Commission threatening much worse legislation if Parliament rejected it again.

The digital revolution does present a real, existential challenge to the Para-state. However this challenge is like an off-shore tsunami, taking place deep beneath the surface, and almost invisible until it is very close by. That makes it all the more dangerous, yet also too subtle to have registered on the radars of our leaders, before the Facebook revolutions of 2011 and later.

Something else happened. It must have been around the turn of the century, and whatever it was, it created enough paranoia and fear to drive major world governments to do some pretty extreme stuff. We're not just talking about good statesmanship and careful preventive action. We're talking about a broad international agreement to disregard the rule of law in the name of maintaining order; specifically, to undermine laws that protect privacy and the freedom to assemble.

There are three main threats that could potentially explain the urgency of the Para-state to build the Spider:

- *The digital revolution itself*, which I discount because the Spider was already assembling by early 2001, too soon to be a response to the growing power of digital society.

115 http://www.zdnet.com/eu-parliament-rejects-data-retention-plans-3039203034/

- *Islamic terrorism*, which we realize today was, and has always been, a bogey man[116]. There is no War on Swimming Pools and Stairs.
- *File sharing* and the threat to the media companies. I would like this answer except that the Spider simply didn't care about file sharing until it was prodded heavily. Perhaps this is because the nerds in the NSA are all too busy downloading Game of Thrones themselves.

It's possible that the threat of international nuclear terrorism was real. Perhaps we are safe and sound thanks to the alphabet agencies, and their careful recordings of our private lives. Maybe. It's hard to prove the negative. I will state my opinion, for the record. That is: the threat of turbaned terrorists nuking our cities and blowing up our planes was an obvious hoax, played by the propaganda arms of our governments on us, the television watching public.

One of the foundation beliefs for the War on Terror is the notion of religion as the basis for conflict. We've been taught that the world is filled with dangerous, angry, and jealous people. They hate our democratic, peaceful, happy way of life. They have decided to destroy it. And that hate, we are told, stems from religion, radical Islam, which is (we are told repeatedly) a nasty backwards philosophy that turns people into monsters.

Now, I've lived for 15 years in a largely Muslim part of Brussels. It's true that there are not many pubs and bars in this area and the cafés are filled with men drinking *café au lait*, rather than beer or wine. We live just down the street from a mosque. It is true that on Friday evenings there are cars parked literally everywhere. I have amicable chats with our neighbors, two Moroccan brothers in their 40's who will occasionally share a smoke with me. I've had pleasant chats with the caretaker at the mosque, a bearded Pakistani man with seven children, about immigrant life in Brussels. My most stressful experience with

116 http://www.washingtonsblog.com/2013/04/statistics-you-are-not-going-to-be-killed-by-terrorists.html

Islam to date was a discussion with a group of kids in the park, who insisted that God was real.

The notion that religion makes men mad is ludicrous. It makes them less sharp, for sure, yet it also has strong survival value for societies in stressful environments. However, our newspapers have been filled with stories of religious wars, extremists murdering women, blowing up ancient monuments, taking hostages, exploding car bombs, and so on.

Let's assume these reports are all true, and not even slightly fabricated, exaggerated, or emphasized. Let's accept that there are no *agents provocateurs*, no secret slush funds to pay armed men to create havoc, no incentive whatsoever for the CIA and its friends to stir up trouble and give it a name and branding. It still doesn't click.

Every violent so-called "religious conflict" is driven by local politics. Northern Ireland, Bosnia, Lebanon, Chechnya, Syria, Algeria, Libya, Northern Nigeria, Iraq, Afghanistan, Sudan, Indonesia, Burma... the story is always one of cynical older psychopaths wrestling for power, using whatever weapons they can, including weak and vulnerable people who can be convinced to fight and die for them. However, if you are in the business of conflict, then sticking the "religious" label onto a political problem does something magical. It makes the conflict unsolvable except through invasion, exhaustion, or genocide. There is no negotiated settlement for a religious war.

It struck me as sinister that in the conflict in ex-Yugoslavia, the three main sides were the Serbs, the Croats, and the Muslims. We didn't speak of Orthodoxes and Catholics, yet in labeling the Bosnians as "Muslim" and casting the conflict as "ancient ethnic rivalries," the world media created the scene for intractable conflict, and arguably, genocide. The actual story was of a group of gangsters who had seized the armory of the defunct Yugoslavia. The thugs then went empire building at the cost of their neighbors, mostly farmers and small city folk, who were unarmed and unprepared. All NATO had to do was hit the gangsters hard one time, and they crumbled.

Myths do of course create their own reality over time. Today there are thousands of young men who have been trained in killing in the name of Jihad, in camps and wars around the world. And whenever there is a violent conflict that figures Islam anywhere in it, it draws these men in. This is not, however, an international organization or movement, just a large bandit gang. And to be honest, it is hard to distinguish this gang from one of the Spider's teeth.

I grew up 300 km from the troubles in Northern Ireland, which were portrayed for decades as an intractable religious conflict between Protestants and Catholics. And yet, when people stopped talking about religions, and instead looked at the politics, we found solutions. This is a consistent pattern.

Conflict is always political, yet leaders often invoke religion to bolster their followers, and create more tribalism. Outsiders, searching for simplistic explanations, and possibly arms sales, embrace this rhetoric as reality. As the conflict increases, the religious arguments will definitely increase. However, it's correlation, not causation. And in the end, the solution comes from addressing the original political issues. Until then, and as long as possible, the beneficiaries (war can be incredibly profitable!) will pump up the "irreconcilable ancient hatreds" angle.

And so it goes with the Global Extremist Islamic Threat to Modern Civilization. It appeals to atheists and Christians alike, and provides convenient cover, both for unprecedented profit-taking, and for creating the spy networks. However, a pumped-up threat of crazy foreign religious nuts doesn't explain the breathless alacrity with which the Spider was assembled, starting in 2000 or so. It doesn't explain why the US government threw away its own rule book on spying on its citizens, why the UK wanted that DRD so badly. As for why the rest of Europe went along without hesitation, perhaps the timing of the London bombings had something to do with it.

The Unmentionable Canary

Child porn is the unmentionable canary in the coal mine of privacy. As much as we may detest child porn, and I do, the crusade against it smoothly morphs into a general crusade against obscenity[117]. This brings us back to censorship, regulation of morality, and the expansion of criminalization. Though it's easy for the authorities to claim, as UK Prime Minister Cameron did, that "on-line pornography is eroding childhood," this is frankly an appeal to laziness and the most negative emotional responses to a serious social problem.

My three children have ranged free on the Web since they could click a mouse, at the age of two or three. We have no Internet filters at home. There are many noxious places on the web, not least inane Flash games that somehow always end up asking for credit card details. My children, even young, have learned that there are dangers out there. It's no different than the dangers of the real world. Strong children are not those who grow up in safety helmets.

The right approach for parents and schools is to actively guide children away from dangerous places — and to explain why — and towards safe places. It doesn't take a genius to realize that if pornography is banned or hidden, it simply boosts its appeal and makes it harder for parents to take control. I'd much rather my son stumbled across a porn site while using the PC in the living room than while at a friend's house.

The creation of the "family-friendly Internet" is a slippery slope, with the obvious, and I assume intentional, outcome of creating an Internet too feeble to hurt the Para-state. First, it's the child porn networks. Then, it's obscenity in general. Then it's unmoderated forums, since adults might meet and groom children there. Then the use of on-line aliases, since that's how child abusers hide. Then it's a ban on anti-establishment forums, because terrorists. Then encryption, be-

117 http://www.telegraph.co.uk/technology/internet/10194641/Camerons-crackdown-on-illegal-pornography-criticised.html

cause that allows discussions to happen secretly, because pedophiles. Then unsanctioned software and devices. And so on.

Meanwhile, children won't be protected in any concrete way. Rather, they will be cut off from anything that might teach them important facts about the dangers of the real world. Worse, it will create a generation of criminals who learn how to circumvent the blacklists and break the law to get access to porn. But above all it would throttle the essential freedoms to speak out and organize against the abuses of the Para-state.

Britain often leads the way in the attacks on privacy, which then become wider policy across the world, especially the Axis of English: Australia, Canada, the US, and New Zealand. If Cameron's experiment takes hold, we can expect to see censored Internet access pushed on a wider basis. In fact, Britain is trailing — Australia has had Internet censorship since 2008 and is classified as a country "under surveillance" by Reporters without Borders.

There is no dividing line between "protecting the children" and removing free speech and free access to information. We just have degrees of state intervention. Digital society must be careful about tolerating the criminalization of behavior, such as seeking socially unacceptable porn, that gives the goons an excuse to push the line the wrong way. As with narcotics, the police are not the right tool for public health issues.

Zombie Conspiracies

There is one other global existential threat to our way of life, and I'm not talking about Hello Kitty. I am however talking about peak oil, and the risks it brings for our comfortable holiday society. Bear with me, I'm not a catastrophe fan (we made it through Y2K, so how bad can the future be, right?). However, that doesn't mean that other people are as optimistic as me.

Though the industrial revolution started with coal, today's global economy owes its very existence to long-chain liquid hydrocarbons,

aka "oil." Of the seven largest global businesses[118], six are oil and gas — Exxon Mobil, Shell, Sinopec, BP, CNPC, Aramco — plus Walmart in position three. Eighteen of the top 50 businesses are oil and gas.

Oil is a funny thing, and I mean apart from the fact that it's about 10 million times cheaper than scorpion venom[119]. Without it, we wouldn't have an industrial society at all, and no digital world either. One could argue that by definition, our species would have found *some* form of cheap energy, thanks to cost gravity. Or alternatively, that by sheer luck and chance, we hit oil just when coal started to become too costly and dirty. Either way, oil is the lifeblood (though about 500 times cheaper than human blood, after the processing fee of $1,500 per gallon of blood is factored in) of our industrial society. Take away oil, and we have some really big problems.

And, although it has dropped off the radar[120] in the last years, peak oil is a fairly solid thesis. That is, we're ending the era of cheap oil, and the future is one of rising oil prices, scarcity, and (more) wars over oil. Deja vu, anyone? We're going to end with Mad Max and large men in weird masks chasing us down the road so they can cut our faces off. The future is scary!

Whether in 50 or 100 years, it's clear that oil is peaking, cheap oil supplies are running out, and the world will change forever as a result. It is difficult to overstate the impact on society as we know it. Our modern sprawling cities, energy-greedy economies, and political systems all grew in the bath of cheap energy. Modern representative democracy — one adult, one vote — was born alongside with the motorcar and cheap petrol. Remove the petrol and the motorcar, and what happens to the political system?

Personally, I'm sure we'll shrug it off. Democracy seems largely a puppet show anyhow. We don't actually need cheap private transport to create an educated and representative society. In fact, cheap energy

---

118 https://en.wikipedia.org/wiki/List_of_largest_companies_by_revenue

119 http://www.cockeyed.com/science/gallon/liquid.html

120 http://www.google.com/trends/explore?q=peak+oil#q=peak%20oil&cmpt=q

may be making us stupider; it certainly makes us greedy and wasteful. Perhaps a world where we're forced to chop and carry our own wood once more, where cities are built to a human scale, and where the night skies are dark, would not be so bad. An extra hour of sleep every night would not hurt.

Further, technology never runs backwards. Cost gravity means that what is expensive today becomes cheap tomorrow, with the arguable exception of scarce natural resources. One example: solar technology, which today is still a luxury good. Thank you, oh patent system! Tomorrow, it will be as cheap as paper and we'll wallpaper the deserts with black panels and connect them with cheap superconducting grids. Oil will run out, and no one will notice except the oil industry. And that industry will have to stop its sabotage of the solar and wind energy sectors, with patents and lobbying, and instead embrace the future.

Does industrial society's political elite see things like this? Do they have such a positive, optimistic view of humanity? I doubt it. The powerful never sees others as good, only as cheap. In 2000, just after the turn of the century, fuel protests broke out across Europe. The BBC reported[121]:

> *Protests over high fuel prices have been gathering momentum across western Europe. Lorry drivers, farmers, and other fuel users have blocked oil installations and disrupted traffic in towns in Germany, Britain, Belgium and the Netherlands. Although nearly all the blockades which crippled France last week have now been lifted, elsewhere protesters have been encouraged by the concessions their French counterparts won. The UK Government has been given authority to take emergency powers to ensure fuel distribution, after the blockade and panic-buying by motorists led to many petrol stations running dry.*

121 http://news.bbc.co.uk/2/hi/europe/919354.stm

Note the apocalyptic tone of this report. I can almost imagine the voice coming from a crackly black and white radio. An elegantly understated 1970's BBC accent reads us the collapse of civilization. "Paris has fallen. Madrid has stopped broadcasting. Berlin is off the air. We are alone. God save the Queen." The last survivors (all white and male, with one token dark female person to show our calculated empathy for the masses) huddle in a bunker. We pray the government will reorganize itself and send in the army to save us. It is one of those old British sci-fi movies, *Day of the Triffids*, perhaps, or *28 Days Later*, with its flesh-eating zombies.

The price of a barrel of oil at the time was $35, a shocking three-fold increase in just two years. As Wikipedia tells it[122], the COBRA committee[123] drew up plans to bring the military into play. When the men in charge put soldiers on the streets, it means they are afraid for their survival. Remember this, America, when your police strap on their body armor and climb into their IED-proof armored vehicles.

I'm no psychologist and the political elite of 2000 did not write blogs to explain their views of the world, so I can only guess how London, Paris, Moscow, and Washington reacted as they saw Europe head towards fuel starvation and civil collapse. *Three questions for the experts. One: How high will oil prices go? Two: How will our citizens respond? Three: What do we do to keep order?!*

And the answers came back. *One: Very high. This is just the start; expect to see oil at $100 a barrel a decade from now. Two: Bloody panic and rioting in the streets. Have you not been following the news? Sheesh! Three: We'll come back with a full proposal. It won't be cheap, although better safe than sorry.*

Our political elite is not selected for general intelligence. They are good at collecting money and power and holding onto it at any cost. That is their skill. Understanding the real world, being good at math, knowing the difference between astronomy and astrology... that's

122 https://en.wikipedia.org/wiki/Fuel_protests_in_the_United_Kingdom

123 https://en.wikipedia.org/wiki/Civil_Contingencies_Committee

what consultants are for! And this elite gets its view of the world from Hollywood. When they watch zombie movies, where the infectious undead ravage our cities and bring down civilization, they don't think "fantasy." Rather, they think "scary metaphor" or quite possibly, "graphical prediction."

My imaginary experts predicted that, in 5 to 10 years, the fuel crisis would cause civilization to collapse. First, the cities would become free-fire zones, infested with drug addicts and cannibals, maybe even flesh-eating multicultural zombies. The army — solid men of many colors, slow, and dedicated — would erect barbed wire fences. And the zombies would inevitably climb over the barricades, and groan and lurch their way to the suburbs. There, the survivors — all white, good teeth — would succumb. Eventually the Vice President would have to nuke half the country just to maintain order.

It would be rather simpler, and less painful, to take measures now.

This is how I figure our political elite analyzed things. Disaster is inevitable unless strong measures to keep control could be taken. And so since 2000, we've seen a wide range of extremely intrusive measures that all have echoes of collective desperation. It's as if, with one mind, the leaders of the free world had decided to dismantle privacy, adopt the most cynical measures to watch every aspect of their citizens' lives, and to hell with legality and the consequences.

Today, as my imaginary experts predicted, oil is three times the price of 2000, at about $100 a barrel. The price is still rising though not as fast as it might be. There have not been any more riots or disturbances over oil — though France did erupt in early 2013 over the unacceptable equality of marriage — and we seem to have forgotten the events of 2000. That was *before Facebook*.

Paranoia sleeps with both eyes open, though. We've only accepted rising fuel costs because the Internet and global trade somehow kicked the world economy back into gear after 2000. Miraculously, the flood of cheap goods from Asia lowered the cost of living enough to compensate for rising fuel costs. That flood can't be infinite. It will

end some day, and then we'll be back to barricades, Molotov cocktails, and zombies.

Meanwhile, the political elite needed something solid to justify their plan to put a ring of iron around their citizens. Which brings me back to our Bogeyman.

Footsteps in the Blood

I find it remarkable how the march of Islamic terrorism seems directly linked to the price of a barrel of oil.

The twenty-first century recycled the term "terrorism" into something quite new. Before 2000, "terrorists" were always groups of angry and violent fighters representing suppressed minorities fighting for a homeland or change of government. We had terrorism in Northern Ireland, the Basque region, Palestine, Sri Lanka, Kashmir, Algeria, Indonesia, and so on. They were always heroic figures, if you liked that kind of thing, though murderous, so you could support either side and still feel good about it. Viva Che!

In September 1999, a series of explosions hit apartment blocks in Moscow[124]. Journalist Alexander Litvinenko[125] was an officer of the Russian FSB secret service (ex-KGB) who first fell out of favor for accusing his superiors of assassinating the oligarch Boris Berezovsky. Litvinenko claimed the FSB carried out the Moscow bombings, which were the excuse for the second Chechen War. He was murdered in London by an unusual radioactive isotope. Anna Politkovskaya[126], another Russian journalist who made the same claims, was murdered in Moscow in 2006.

We know how the events of September 11th changed the world. The US government pulled the PATRIOT Act out of the drawer, pushed it through into law, and proceeded to invade Afghanistan and then Iraq on the pretext of hunting down the terrorist perpetrators. Most

124 https://en.wikipedia.org/wiki/Russian_apartment_bombings

125 https://en.wikipedia.org/wiki/Alexander_Litvinenko

126 https://en.wikipedia.org/wiki/Anna_Politkovskaya

of the rationales for those wars, such as Sadam Hussein with his anthrax factories being behind the 9/11 attacks, and building weapons of mass destruction, turned out to be false.

What fewer people know about, or remember, is the murky behavior of the US government before and after the 9/11 attacks. The New York Times wrote, in September 2004[127], how the FBI refused "to allow investigators for a Congressional inquiry and the independent Sept. 11 commission to interview an informant, Abdussattar Shaikh, who had been the landlord in San Diego of two Sept. 11 hijackers." According to the Co-Chair of the Congressional Inquiry into 9/11, former Senator Bob Graham, also a former chairman of the Senate Intelligence Committee, "this cover-up goes right to the White House."

Graham went further[128], alleging that "in the final report of the congressional inquiry, there was a chapter related primarily to the Saudi role in 9/11 that was totally censored, every word of the chapter has been withheld from the public. Some of the other questions we ought to be asking are if we know that the Saudis who lived in San Diego and now apparently in Sarasota received substantial assistance, what about the Saudis who lived in Phoenix, Arizona? Or Arlington, Virginia?"

Unfortunately, any suggestion that 9/11 was predictable, or allowed to happen[129] by negligence, or even made to happen, is to be branded a conspiracy nut[130]. The mainstream media did not then, and still does not, look at any details that contradict the official story. To question the mythos of the War on Terror is literally to risk indefinite detention in a psychiatric ward[131].

127 http://www.nytimes.com/2004/09/08/politics/08graham.html?_r=0

128 http://www.rawstory.com/rawreplay/2011/09/former-sen-bob-graham-calls-for-new-911-investigation/

129 http://www.washingtonsblog.com/2011/08/bush-and-clinton-counter-terrorism-czar-alleges-massive-911-cover-up.html

130 https://en.wikipedia.org/wiki/Richard_A._Clarke

131 http://www.washingtonsblog.com/2012/08/former-locked-in-psychiatric-ward-over-his-911-facebook-posts.html

The line of evidence connecting 9/11 to the Spider's growth may be thin, yet is one of the clearer trails in a chaotic mass of lies, omissions, bluffs, and misdirections. As the Raw Story reported in 2009[132],

> *Author James Bamford looked into the performance of the NSA in his 2008 book, The Shadow Factory, and found that it had been closely monitoring the 9/11 hijackers as they moved freely around the United States and communicated with Osama bin Laden's operations center in Yemen. The NSA had even tapped bin Laden's satellite phone, starting in 1996. Not only was then-Director Michael Hayden never held accountable for the NSA's alleged failure, but he went on to oversee the Bush administration's vast expansion of domestic surveillance. In 2006, he was appointed as director of the CIA.*

For the sake of argument, imagine the most powerful men on the planet coming out of the post-Cold War security services. Vladimir Putin was in the Russian KGB for 16 years[133] before retiring to move into politics. Though George H. W. Bush was director of the CIA for just over a year, Russ Baker claims in Family of Secrets[134], with much research, that the Bush family played a central part in US politics and secret services for half a century.

These men had made phony war their business for decades, and ran the largest budgets in the world, so when their era of "mutually assured destruction" ended, they were presumably looking for new work. I would, in their place.

I think that by the end of the last century, Islam was selected as the best candidate for a Bad Guy to replace the crumbling East-West divide with its slowing profits for the military-industrial complex. We have the mass immigration of North Africans and Turks into Europe as the basis for anti-Islamic public policies in Europe. We have the

132 http://rawstory.com/news/2008/PBS_NSA_tracked_911_hijackers_but_0127.html

133 https://en.wikipedia.org/wiki/Vladimir_Putin

134 https://en.wikipedia.org/wiki/Family_of_Secrets

conflicts in Chechnya, Indonesia, India, Afghanistan, ex-Yugoslavia, and of course, Palestine, to prove how Islam is the religion of hate.

We had at least $600 million[135] of American money going to Gulbuddin Hekmatyar, the founder of the Hezb-e Islami radical Islamic militant faction. Hekmatyar worked closely with bin Laden, and then received further money from the Saudis, close friends of the Bush family for decades, and the home country of the 9/11 hijackers. Hekmatyar was just one of many warlords and pirates to accept illicit slush money in return for violence against America's enemies. Remember the Iran-Contra affair?

Oil, Saudi Arabia, Afghanistan, intractable religious conflicts, NSA, CIA, KGB, exploding tower blocks, ex-secret service men becoming presidents, terrorists-for-hire, and a new War on Terror. It works very well as a story arc. Whether it's true or not, history will discover. What is certain is that a lot of tax and oil money went to building up a credible Islamic threat in Afghanistan. And then a whole lot more was spent on fighting it. And during that fight, we slipped and broke our civil liberties.

In the late 1990's, we were expecting the "peace dividend" and the downsizing of our armies and secret services. However, the security money train did not stop or slow down. Instead, it almost doubled in size[136] during the first decade of this century. We thought we had left the destructive wars of the twentieth century behind us, and instead we find that in this century, we were always at war with Eurasia.

The defining feature of the Para-state, apart from their belief that B-movies are honest-to-god documentaries, is their inability to connect with the majority. Spend a weekend in a luxury hotel, all costs paid, and you will feel superior to the bellhop. Be born into a life of privilege, where luxury hotels are for the poor and outcast, and you will know to the core of your being that you are a god walking among mortals. And gods answer to no one, except perhaps higher gods.

---

135 https://en.wikipedia.org/wiki/Al-Qaeda#Jihad_in_Afghanistan

136 https://www.cfr.org/defense-budget/trends-us-military-spending/p28855

Follow the money. On the one hand, you have a political elite who are convinced the world is about to end if they don't take drastic action soon. On the other hand, you have a military-industrial complex not so keen on retirement and a 75% cut in income. And on the third hand, you have a compliant public with savings, pensions, and a shockingly innocent trust in their rulers.

So a terrorist threat created and pumped up entirely to satisfy a paranoid elite's need for an external threat is not far-fetched. It is one of the simplest plausible explanations for the whole circus. It's exactly what I'd do, if I were an ex-CIA officer. A possible flaw in this reasoning is that it assumes a certain level of competence I'm not sure our intelligence services possess. Still, Iran-Contra shows that real conspiracies do happen in our governments.

The Ring of Steel

Arguably the most spied upon country is the Nanny State, also known as the United Kingdom. In March 2011, a study by the Cheshire police estimated 1.85 million CCTV cameras nationwide[137]. Two years later, a study by the British Security Industry Association came to a figure of between 4 and 6 million[138].

The London Tube is widely reported to be covered by 11,000 cameras, which is about 40 per station. That seems like a low estimate. If you visit busy stations like Kings Cross, you can see dozens of cameras covering the turnstiles and stuck to the roof like colonies of hanging fruit bats.

The London "ring of steel"[139] was originally built to defend against IRA attacks on the capital. It has morphed over time from physical measures against car bombers to today's all-seeing blanket of cameras.

---

137 http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance

138 http://www.securitynewsdesk.com/2013/07/11/bsia-attempts-to-clarify-question-of-how-many-cctv-cameras-in-the-uk/

139 https://en.wikipedia.org/wiki/Ring_of_steel_(London)

Part of the infrastructure came together with the congestion charge[140] in 2003, which gave the city the motive and opportunity to track every car's movement. At the time, tracking cars by reading their plates was cutting edge technology. Today it's cheap and widespread. If you drive, you are tracked.

On CCTV, Privacy International says[141]:

> *CCTV is a seductive technology. In a public policy domain which is notoriously rubbery, CCTV has a solid, "Sexy," and powerful image. It has become an icon for security and — for politicians — its promotion is guaranteed to create a feel-good response. When people are frightened of crime and criminals, critics of CCTV are often portrayed as enemies of the public interest. While Britain is clearly the lead nation in implementing CCTV, other countries are quickly following. North America, Australia, and some European countries are installing the cameras in urban environments which a few years ago would most likely have rejected the technology.*

In the US, terrorism and crime are used as the plausible explanations. A 2007 CNN story[142] about "the 'Ring of Steel' coming to New York" mentions "terror" seven times. The proposed surveillance system consists of license-plate readers, as refined in London, and CCTV cameras. In continental Europe, crime is the main rationale. Previously colorful districts of Brussels, like the African Matonge area, are now monitored by high camera towers. The petty drug dealers are gone, and so are the undocumented immigrants and the nightlife.

Yet except for a small section of alarmists, and perhaps anthropologists studying inner city diversity, the public does not seem worried. According to CNN again: "a majority of Americans said they approved of the use of surveillance cameras by nearly a 3 to 1 margin in a

---

140 https://en.wikipedia.org/wiki/London_congestion_charge

141 http://www.privacyinternational.org/issues/cctv/

142 http://edition.cnn.com/2007/TECH/08/01/nyc.surveillance/index.html

recently published ABC News/Washington Post poll." Security does not just trump Liberty, he takes her into a dark back alley, violates her repeatedly, and then beats her senseless with a heavy stick.

How effective is the surveillance? The CNN article quotes Steve Swain, who was a Detective Chief Superintendent with the London Met Police Counter Terror Unit (PICTU) during the time of the September 11th attacks, as saying, "I don't know of a single incident where CCTV has actually been used to spot, apprehend, or detain offenders in the act. The presence of CCTV is irrelevant for those who want to sacrifice their lives to carry out a terrorist act."

That's a fairly damning critique, yet it only applies if the goal really is to stop terrorism. If the goal is simply the removal of privacy so we feel intimidated and less secure about engaging in political protest, then the cameras and car tracking are working precisely as planned. Hence the cultural death of Matonge, which was a center for political protest about Europe's policies in Central Africa.

Surveillance in the real world keeps track with its digital counterpart. The only restraining factor in both cases, as far as we can tell, is cost — not legality, ethics, public opinion, or benefits. The cost will continue to fall, and the number of eyes will continue to double every two years. Fixed cameras will give way to smart cameras that move and zoom to track pedestrians and car occupants. The eyes will shrink to just millimeters across and find their way into the very infrastructure of the city — street lamps, traffic lights, stop signs. They will grow legs and scuttle around in corners, get wings, and fly around like little insects, tracking interesting people and cars.

Every new train, bus, and taxi already has surveillance in the name of security. The cameras now have microphones, so what you say in the back of the taxi can be recorded. Vast amounts of data are processed by private firms, shared between agencies, and tied into the digital surveillance network. When your Facebook profile meets a suspect, the Spider sees it. And of course to offset the huge cost of this surveillance, it makes sense to sell the data to private firms or give

them the contract to collect and resell it for sales and marketing purposes.

Today, we're still safe inside our homes and offices. I think it's just a matter of time until that changes, unless there is a dramatic change in public attitudes towards being watched by the gray men, which I think is unlikely. I'm not sure what the arguments or events will be that convince us to invite the gray men over our doorsteps and into our homes. Maybe they won't even ask. They will just silently turn on the microphones and cameras in our laptops, or hack into the "always on" cameras on our entertainment systems and smart TVs.

As Sean Hollister asks in the Verge[143], "Will the NSA use the Xbox One to spy on your family?" noting that despite denying it was even technically possible, "Microsoft gave government agencies access to private Skype video and audio calls, perhaps even going so far as to integrate Skype into the NSA's controversial PRISM surveillance system."

The change could come when they convince us that they need to "protect the children" or "provide security services to the elderly." It could start with some vulnerable section of the population such as criminals who are on parole, or drug users in rehabilitation. It could be drones that fly down streets, looking inside windows and through curtains. It's only cost and technical difficulty, both rapidly eroding, that stop the ring of steel around us from growing faster than it does.

The Price of Privacy

In a telling YouTube video, a young man takes a video camera and simply records people in public[144]. He walks up to people, starts filming, and when they complain, he points out that the streets are filled with CCTVs already. He gets some very angry responses. We certainly do care when individuals invade our privacy.

---

143 http://www.theverge.com/2013/7/16/4526770/will-the-nsa-use-the-xbox-one-to-spy-on-your-family

144 http://www.youtube.com/watch?v=cPr2SKf2fXo

However, when it comes to the destruction of our privacy by the alphabet agencies, business, or criminals, digital society has mostly responded with resounding silence. It has been over a dozen years since the Qwest incident, and yet it's only in 2013 with the Snowden leaks that the Spider is making headlines. The shock is not that the Spider is tracking our every word and deed. The shock is that people were surprised by this.

I'm going to try to understand why. I think a number of factors explain why we tolerate the spying eyes:

- *We are being boiled like frogs.* Instead of sudden changes, we experience many small adjustments, each with a plausible explanation. There's always a carrot, and a stick, for every small shift. After many years, we don't just accept the system; we are emotionally invested in it and defend it. After all, the alternative would be self-humiliation.
- *The young man was just being rude.* You can film people in public if you're polite and convincing about it. He should have said, "I want to record you for this series I'm making about privacy, do you mind? If you don't like it, I'll go ask that other guy."
- *We feel we're getting a good trade.* Sure, Facebook knows a lot about us, yet we also learn a lot about other people. Sure, websites track us with cookies. Oh look, pretty pictures!
- *We enjoy the attention.* Most people are pretty lonely, and the idea that someone is watching isn't half as scary as the alternative — that no one cares. This is why many people enjoy getting some spam. It may be junk, yet at least it's coming to us, personally.
- *We calculate that it doesn't really matter.* We tolerate the cameras and spying because we know it's security theater, and we're not really that dumb to take it seriously, even if we like to pretend we are.
- *TV taught us that privacy is a bauble to be traded for a few drops of fame.* Tell the world your most intimate details, and become a

star for 15 seconds. Famous people don't have privacy. Why should the rest of us need it?

- *The bogeyman will get us if we argue.* This still works with many people, though fewer than before. You can only cry wolf a few times before people switch off.
- *We simply don't think about it.* As with any bad news that affects us all, be it climate change, nuclear meltdown in Japan, rising fuel prices, deforestation, pollution, and so on, we deal with it by making it someone else's problem. Sure, it's bad, yet it affects so many people. So someone else will fix it.

It's much like airport security, which everyone knows is pointless and annoying theater. We tolerate it unless it makes us miss our connections, because it's more fun than being ignored. Airports are frankly boring places. If every street-smart flier complains about the TSA, isn't that just because some people enjoy complaining? The ritual of checking papers is a comedy that makes many people feel a little better.

I think when we lived small lives, our secrets were more precious. At some level, we knew that privacy was a luxury and a relatively recent one. People used to live, and still do in many places, in cramped, smelly villages where everyone knew everything about everyone else. So today we're in the global village, and all the walls are grass again.

The Naked Future

In this chapter, I've documented how the Spider, those faceless alphabet agencies of the state, is spying on us. Our current web architecture, built on centralized servers, accessed through commercial broadband links, is trivial to tap. I've explained how the cost of storing everything interesting about us is falling down to zero.

As to the "why," we see the Para-state — a paranoid global political elite fighting to hold onto power — prodded by a military-industrial complex that was running out of enemies before the terrorists, drug cartels, and on-line pedophiles conveniently came along. It doesn't

even require a conspiracy. The collapsing cost of storage and computing power, combined with the centralized Web, makes global surveillance an inevitable outcome.

No matter what the shocking revelations, no matter the public outrage — it is simply too easy to spy on our electronic lives and too costly to prevent it. To some extent, society has accepted this as a fact of life and has become inured to it, even embraced it. We discount our own privacy so our secrets become worthless.

The real question is not whether the total loss of privacy will happen, nor even how long that might take. In many ways, the war on privacy is the bogeyman, scary and yet inevitable, and thus ineffectual. The real question is what impact it will have on digital society, and how digital society will respond, force against force. Before trying to answer that, I need to first look at the wealth and assets of digital society, as that is where its power stems from.

Chapter 6. Wealth of Nations

It owned all the lands, the wealth beneath, and the wealth above.

After the heady mix of paranoia and drama from the last two chapters, let's look at something more sober and calming if not downright boring: wealth and property. These, like freedom and privacy, only make sense in the context of other people. Property is the main reason the State exists at all. The State defines property by law, and enforces its law through courts to create a free market. It builds its economy on the resulting market and derives its power from that economy.

It was always so. To control England after their invasion, the Normans set a lord in a castle on each piece of land, extracting a yearly quota of knights or taxes. Land was the seat of feudal power. This lasted until the seventeenth and eighteenth centuries, when international trade became more profitable than agriculture. By the nineteenth century, the new industrialists took control of politics across the world, and the rural landowners were slowly impoverished.

In this chapter, I'll start by exploring what wealth really is, where it comes from, and where it's going in our digital world. On the way, we'll see why governments and property laws exist at all, and why some forms of property, like patents, make us poorer instead of wealthier. I'll try to answer the question, "How much is digital society worth?" Finally, I'll try to convince you that the new wealth of digital society presents an existential threat to industrial politics.

The Culture seemed harmless. However, the Empire depended on its vassal masses. If these left to go to the Culture's cities, the Empire would starve, and it would die.

In Search of Meaning

The dictionary definitions of wealth and property are, if technically accurate, devoid of any deep meaning. Wealth, we're told, is the abundance of possessions or money, or the state of being rich. Even without pausing for breath, I know this to be wrong by omission. What about knowledge and skills? Family? Friendships, contacts, business relationships, secrets, status, good genes? And who or what defines value?

As with "freedom," my intent is to dive below the surface so we can see what's going on. Without a deeper meaning, we float on the surface with no clue as to the currents below. Like freedom, "wealth" and "property" only have meaning in terms of other people. Let me thus provide some simple yet functional definitions. I'll use these as the theoretical basis for the rest of the chapter:

- *Assets* are things you have that are valued by other people. Assets can be tangible or intangible, more or less convertible, more or less portable, and so on.
- *Property* is the exclusive right to control some assets. Property can be owned by individuals or groups. It can be backed by the authority of the State, or by other means.
- *Currency* is a form of property that society accepts at the present time, as a medium of exchange. It is synonymous with "money."
- *Wealth* is the balance of our assets minus our liabilities.

In some cases, property and the underlying asset are the same thing. In other cases, the differences are profound. Although people are usually assets, they are not, generally, property. Though more money can make us wealthier, some assets, like family and friends, are much more valuable. A lonely man with a lot of money is not wealthy.

Some other terms I'll use are *convert*, *transfer*, and *trade*. We convert assets into other forms and acquire property by transfer or trade. For example, my assets include my time, talents, expertise, and good health. I can convert these into currency by working for others. With

that money, I can buy a month's exclusive use of the apartment I rent, which is an asset.

Over time, societies may collect more accurate knowledge and truths, more people, and more arable land. They may build up infrastructure, cities, markets. They may discover more natural resources. All these will add to their wealth. They may also lose forestation, topsoil, people, knowledge, and thus become poorer.

We can measure a society's success objectively by looking at countable indicators of the quality of life: life expectancy, working week, levels of violence, levels of illness, and suicide. Would you rather live longer or have more money? Even my children know the answer to that one. By such measures, global human society is becoming wealthier. World average life expectancy in 2010 was 67[145], while a hundred years ago, it was 31, up from 20 in the Neolithic, 28 in classical Greece and Rome.

Why the State Exists

A classic libertarian argument is that the State, though evil and expensive, exists because it is too powerful to remove. I'd like to put people who seriously believe that into a stateless region of the world for a week or two, such as Lebanon in 1980, Somalia in 2000, or any major slum that the police do not patrol.

The State is a human universal because it answers an old problem in the simplest and usually cheapest way. This core problem is that we men (I can't speak for women here) argue and fight over access to females, territory, status, and property. As a matter of survival, we don't back down from fights unless we're entirely outmatched. Further, when someone attacks us, the winning strategy is to hit harder, not retreat (again, unless we're outmatched). This entirely logical strategy has a disastrous outcome. Small arguments escalate into major tit-for-tat violence, until one side is too weak to fight anymore.

---

145 https://en.wikipedia.org/wiki/Life_expectancy

It's this simple dynamic that powers many civil conflicts between previously peaceful neighbors. It can turn small arguments into nationwide destruction, as we saw in Lebanon from 1975 to 1990, or Somalia from 1991 to the present day. Such conflicts can be impossible for outsiders to understand because they occur between clans and fluid extended families, rather than political blocks. One feature is consistent, however: the lack of a State strong enough to intervene with force.

The State grants itself a monopoly of force, which it uses to define a set of laws and enforce them through criminal and civil courts. If a family squats on another's land, the State will evict them, not the owners. If one man shoots another dead, the State will punish him, not the dead man's family. If a man rapes a woman (arguably a form of theft), the State will prosecute him, not the woman's family.

Laws, courts, and police are tools for reducing violence by intervening in conflicts at the earliest possible moment and punishing the aggressors. To be utterly cynical, it doesn't really matter who is innocent or guilty as long as there is no option for either side to take matters into their own hands.

A successful State reduces violence over time, and thus we tolerate it and pay for it. Even a State that steals from its people on a massive scale — like the Para-state — is better than no State at all.

Arbeit Macht Frei

I'm a firm believer in the free market. I'm not a fan of free market economists. Here is how Wikipedia sums up[146] the free market view of private property rights:

> *According to the free market view, a secure system of private property rights is an essential part of economic freedom. Such systems include two main rights: the right to control and benefit from property and the right to transfer property by voluntary means. These rights offer people the possibility of*

146 https://en.wikipedia.org/wiki/Economic_freedom

autonomy and self-determination according to their personal values and goals. Economist Milton Friedman sees property rights as "the most basic of human rights and an essential foundation for other human rights."

With property rights protected, people are free to choose the use of their property, earn on it, and transfer it to anyone else, as long as they do it on a voluntary basis and do not resort to force, fraud or theft. In such conditions most people can achieve much greater personal freedom and development than under a regime of government coercion. A secure system of property rights also reduces uncertainty and encourages investments, creating favorable conditions for an economy to be successful.

Empirical evidence suggests that countries with strong property rights systems have economic growth rates almost twice as high as those of countries with weak property rights systems, and that a market system with significant private property rights is an essential condition for democracy.

According to Hernando de Soto, much of the poverty in the Third World countries is caused by the lack of Western systems of laws and well-defined and universally recognized property rights. De Soto argues that because of the legal barriers poor people in those countries can not utilize their assets to produce more wealth.

It sounds sensible, doesn't it? The theory of strong private property rights, as the basis for democracy and prosperity is attractive. It appeals to our self-interest and seems to fit the empirical data. The West emphasizes private property, and also has successful economic systems and democracy. The US takes this theory to the extreme, and is the wealthiest, most democratic nation on earth. Surely this proves the theory.

To nullify any theory, it's sufficient to find a single exception. So let's take a secure system of private property rights that breaks this theory. For hundreds of years, on and off, the West had a property system called "slavery," which allowed one person to own another. It was a very strong system of rights, backed by law and the full force of the State. It made many very wealthy, and the proceeds of slavery were arguably the seed capital for the industrial revolution.

Yet we abolished slavery, and few would argue that abolition was a mistake. Why did we abolish it? Certainly the work of abolitionists in uncovering the hidden costs of slavery was crucial. However, the end of slavery in the Americas came, I think, simply because it did not work very well as an economic system, once mechanization ended the profit margins on manual labor. Cost gravity, again. However, even disregarding mechanization, slave societies are poor relative to societies where everyone is free to contribute, and where no infrastructure of repression is needed.

The Union beat the Confederacy in the US Civil War not because of superior strategy, or better generals, or the Will of God. It was simply much more powerful. Its free market attracted more immigrants, and gave them more freedom to organize socially and economically. It had better infrastructure. It could produce weapons, medicine, and soldiers significantly cheaper than the South could. It could build and maintain a powerful navy. In a war based on slaughter, the South could simply not keep up with the industrialized economy of the North.

The US does have a large free market, and it benefits greatly from immigration and the control of abundant natural resources. Its military spending is more than that of the dozen next biggest spenders combined. However, the US is like a lonely rich man: wealthy in some respects, painfully impoverished in others.

The US ranks 33rd in global life expectancy[147], neck-and-neck with Cuba. It actually sits right between the western European countries, all in the top 30, and those of the ex-Soviet block, that follow it.

The centuries-long experiment in capitalism has thus produced clear empirical results. US worship of strong private property rights beats slavery, yet is barely better than Soviet-era central planning. If the proof of the pudding is in the eating, the right-wing economists are chewing on something cold and rubbery.

The blind worship of strong private property rights has allowed many abuses. Broadly, it is an excuse for the rich and powerful to steal public assets and then claim they are the "wealth creators." It has been the plank for many a coup, invasion, and even genocide on grounds to stop "socialist" regimes and their "mad" policies. It blessed the "greed is good" mantra that eviscerated business ethics in the last decades. It protects the patent system from scrutiny and gives it space to grow. It is the curtain that hides the malevolence of the Para-state.

And it is fundamentally and powerfully wrong. Wealth does not come from creating more private property. *Wealth comes from other people.* It is true that the concept of property can protect, capture, and carry that wealth. Yet, property does not create wealth any more than a bucket creates the water it holds.

How could so many leading economists be so wrong? The US should be heaven on earth and yet is instead tottering towards corrupt totalitarianism. It is becoming a crony State run by and for billionaires, no matter the cost to wider society.

Let's look at the theory again, specifically its notion that a free market is one without coercion. The nineteenth century German economist Prince-Smith wrote, "*Any claim for protection of private property is a demand for the intervention of the power of the state.*" Private property can *only* exist thanks to government coercion of one kind or another. Some forms of private property, like slavery, or pat-

147 https://en.wikipedia.org/wiki/List_of_countries_by_life_expectancy

ents, have very high coercive costs. A "free" market is not one without coercion. It is one where the coercion is accurate and fair.

And here we come to the core flaw with the theory. It claims that private property is always good, and public property is always bad. It claims we will not invest unless we can own the results privately. It was Margaret Thatcher's belief that "there is no such thing as society. There are individual men and women, and there are families" cast into economic policy.

I've shown in earlier chapters how we humans can be extraordinarily good at working together. Not only is society real, it defines the human experience. We invest in public assets for entirely selfish reasons on such a massive scale that it takes a special kind of blindness not to see it. Any large-scale investment needs the right mix of public and private assets. Observe the Internet — the largest and most effective global infrastructure ever built — constructed as millions of private properties built on public assets (its standards and technologies).

In fact, an efficient free market absolutely depends on public assets. If you privatize the playing field, the owner will tilt it in his favor[148].

All law is an answer to a set of problems. Stronger private property law is a brilliant, rational answer to the wrong problem: how to encourage individual investment and how to allow the wealth creators to escape the shackles of a parasitic society. The actual problem is: how to protect real investments from cheats (both the skinny beggars and the fat bandits).

As I showed in the story of sub-Saharan Africa, endemic poverty comes from distant, fragmented, and unfair markets. No stronger property laws will open more ports, move Africa closer to Europe, or break the grip of the criminal elites and their foreign allies. In fact, the demand for "strong property laws" can have the perverse effect of privatizing common assets such as plant genes, malaria research, and natural resources — in effect destroying, not creating, wealth.

148 https://www.google.com/search?q=railroad+barons

Congo-Kinshasa, one of the wealthiest nations on earth in natural resources, ekes out a life expectancy of 49 for its citizens, third last out of 193 countries. Yet it has some of the strongest property rights imaginable, for the friends of the regime.

Strong private property laws are an outcome — not the origin — of a successful free market. The economists who developed the flawed theory saw poor countries with weak protection of private property, and assumed this was the cause of the poverty. It fits an anti-socialist political bias and confirms the West's superiority complex. It played into the hands of the wealthy, who got justification for yet more profits. And even economists need their grants, wealthy donors, and tenure. The right-wing economists missed, or ignored, the fact that poor countries were also hostile to trade, with restrictions on travel, poor natural infrastructure, bad communications, monopoly control of the market by state enterprises, and, often, extraction economies.

Property as Game Theory

Perhaps I am being unkind to the right-wing economists, and their confusion of cause and effect. They did get at least one thing right: property laws *do* make a difference. Bad property laws can crush us, and good property laws can raise us up. I'm absolutely a fan of good and fair private property rights. However, I've also experienced, personally, how destructive bad property rights can be.

There is no single law on property. There are many, many forms of property in a modern society, each with their own set of rules. These rules have been worked out by trial and error over thousands of years. However they always have one thing in common: they are written by powerful people for their own benefit. Sometimes that matches the greater good, and sometimes it does not. How can we tell the difference without the trial-and-error that so often results in dire consequences? Did we really need centuries of war in Africa leading to tens of millions dead, and a major civil war in the US to prove that slavery was a bad idea?

If we see property as wealth by definition, it is very hard to say, "There are bad forms of property." That would be like saying, "There are bad forms of money." The notion would be ridiculous. Surely all property is worth at least *something*. Property with a negative value? Perhaps one rotten house, or polluted piece of land, or even a dying city, yes. A whole class of property? Unpossible!

However, if we see property as monopoly control over some assets in order to stop cheats, then we can definitely measure the pros and cons of that monopoly. People are assets, yet there is a profound difference between assigning the monopoly of control over a person to that individual (freedom) or to another person (slavery).

It becomes easier to measure the costs and benefits of property law once we understand creating de jure property titles does not create assets except in a corrupt legal system. Property can be a container for assets. However, those assets exist with or without property law. Let me make this clear by comparing two situations.

- The city owns a large apartment complex built to house poor people. Under a new right-wing mayor, the city sells the apartments to their owners at a low cost. The new owners repaint and repair their apartments, and sell them to others at the higher market price. Have we now created assets? We've certainly created property. However, any assets we've "created" has actually come from someone else's pocket. That is not wealth creation, indeed it is theft.
- There is a shantytown just outside the city, where other poor people built rickety houses. Under a new left-wing mayor, the city grants long-term leases to the inhabitants and provides them with subsidies to buy better materials. It provides water and electricity to the area, creating a new district. The old tin homes start to be replaced with brick houses. Have we created assets now?

So a good form of property is one that wraps up existing investments and assets, and protects them from abuse. It's not the selling of a home at a higher price that creates wealth; it's the building of a

house close to other homes, and the creation of a society. All rules — and especially property laws — must be resistant to cheats. Otherwise, people will not play. When a market tolerates cheating, people work around it and eventually abandon it. A favorite tactic of cheats is conflict and confusion, because in a legal dispute, the more powerful party almost always wins.

A good property rights system steers cheats away and draws in honest investors. It has these features: it gives proportional title over a real investment; it has explicit and unambiguous boundaries; it is cheap or free to acquire the title; it is cheap or free to enforce; it does not conflict with other assets or property rights; and it has a low or negative cost to the rest of society.

By "proportional title over a real investment," I mean that the title should match the investment in a sane way. For example, if I clear one small patch of jungle and thus get title over 10 acres of land, that is disproportionate. If I clear an acre and get title over that acre I cleared, that may be fair.

Nowhere on my list is "encourages investment" because that is a bogus criteria based on a misreading of the human spirit. We compete obsessively, it's in our genes, and we'll simply focus our attention where we think it will pay off best. Artists won't suddenly stop making art because they can't take imitators to court.

For the most part, property systems that score high are never in the news because they simply work. Trademark law mostly works very well. It gives title to existing investments (business goodwill) and has no cost to society, yet protects the investor from cheats. It is cheap to acquire and easy to enforce.

When a property system is often in the news because of lawsuits, that is a good sign that it has problems. Coercion and law only go so far. It is especially significant when you see wealthy lawyers suing ordinary businessmen: this should send alarm bells ringing up and down.

A Rough Timeline of Property

Two hundred thousand years ago, modern humans went hunting and foraging their way around the planet. When your tribe moves on foot from campsite to campsite every few days, physical goods are liabilities rather than assets. You can make new stone tools, shelters, and other necessary things with less effort than it takes to carry them around.

I asked my young daughter this question: "If you were in the park with your friends and you had five ice cream cones, what would you do?" She answered, "I'd share them with my friends." I then asked, "If you had a lot of money, would you share it?" She replied, "Of course not." I then asked, "If you wouldn't share the money, then why would you share the ice cream?" She thought for a while and answered, "Because I couldn't eat it all myself."

Likewise, a successful hunter who has no way to preserve his meat has to convert it immediately by sharing it with others. However, give that same hunter a fridge or a bag of salt, and suddenly he may see the logic of not sharing. We don't need to be taught to accumulate assets or know the difference between dried meat (highly convertible, yet perishable) and social credit (non-perishable, though not convertible).

Ten thousand years ago, we invented the wheel and the ability to carry our possessions around on wheeled load-carriers. Suddenly, our things became assets instead of liabilities. We could invest much more time in tools, weapons, jewelry, clothes, tents. I assume, though can't prove, that property was de facto; you owned what you held, whether you made it, found it, traded it, or stole it. I am absolutely certain that the hours and days invested into a tool or jewelry or clothing or weapons were not treated as disposable.

Four thousand years ago, we invented agriculture and built the first cities and empires. Suddenly, we could accumulate wealth beyond what we could use individually or in a clan. We rapidly invented writ-

ing, number systems, money, de jure property, written laws, courts, and a civil service.

The first currencies were precious objects like cowries[149], or rare minerals like salt and gold. These became symbolized and regulated over time. Gold was shaped into standard bars, marked with the sign of the ruler, then into smaller pieces, then coins of various metals. Eventually these were replaced by paper money.

A currency doesn't have to be backed by the State; however, it must be convertible. A state-backed currency loses value if the State prints too much of it, as States tend to do eventually. A natural currency stops being convertible if it stops being rare. The best currencies are highly portable (I can carry them with me), anonymous (I can spend them without others discovering), and scalable to any size of market.

Two thousand years ago, we invented clean water, hot baths, social security, highways, concrete, and civil engineering, and built continent-wide trading empires. We invented public and private law as the basis for modern legal systems, and the free market. It all went well except for the lead in the water.

Two hundred and fifty years ago, we invented the steam engine and decided it was more profitable to build factories than grow sugar. We invented "intellectual property" on the basis that if we didn't own the ideas in our minds, we would stop thinking.

About five decades ago, we invented the Internet as a few megabytes of technical protocols anyone could implement for free. The notion of open and free protocols was radical at the time. By the end of the twentieth century, investors were pouring billions into businesses whose only model was "spend money." For many people, the main reason to go on line was to download stuff for free and annoy the music and movie industries. Eventually, most people went on line just to meet and talk with other folks, building huge social networks of all shapes and sizes.

---

149 https://en.wikipedia.org/wiki/Shell_money

Some of digital society's most valuable assets are those social networks. You might think they're owned by the businesses that operate them. You're wrong.

The Most Liquid Asset

MySpace (remember that?) had a peak valuation of $12 billion in 2007. To put this into context, the price of land in Paris, France is about $1.2 million per acre (EUR 240 per square meter, according to Pierre-Philippe Combes, of Aix-Marseille University). So the 20,000 acres of metropolitan Paris is worth about $26 billion, not including the infrastructure, buildings, and businesses on that land.

Imagine all of Paris south of the Champs-Élysées and Seine River — 9,000 acres — owned by one company, supporting an immense amount of social and economic activity. By 2006, MySpace had 100 million accounts and was the most visited website in the US, even more so than Google. It wasn't just inhabited by teenage girls. Every musician and his or her dog used MySpace for their fan clubs.

Five years later, in 2011, MySpace was sold for $35 million. In early 2013, its owners launched a facelift that demolished the last remaining buildings and evicted their tenants. Before that, Britney Spears had about 1.5 million friends on MySpace. After, she had fewer than 7,000[150].

An acre of land in rural France costs about $6,500. That puts the value of the 9,000 acres of virtual Parisian soil at about $58 million. In effect, MySpace's various owners managed to raze half a city (and not just any city, the City of Light!) and poison the earth so that it was worth less than empty farmland.

The MySpace disaster is a textbook example of smart people doing stupid things. There are many technical explanations for what went wrong, when in fact it was really simple. Facebook built a better city, and people moved. It took a few years, yet everyone migrated and

150 http://techcrunch.com/2013/02/02/myspace-squandered-the-only-thing-it-had-left/

took their assets — their friends and connections — with them. Facebook is, in 2013, about six times more valuable than MySpace was at its peak.

What we seek, when we move, is a better market for our assets. That is, easier and cheaper convertibility, and better and cheaper authority. This is why the freedom to leave a corrupt authority is so important. It is essentially the only force that promotes honest competition between authorities.

Copyrights

How Good is Copyright Law?

The word "copyright" only makes sense when you prefix it with "exclusive." Copyright gives a monopoly on the right to distribute some creative work. Originally it covered books, and today it covers any creative expression that has tangible form. Like all laws, copyright law comes down to convincing a judge or jury.

From the start, copyright law was about protecting distributors more than creators. An author writes a book, which is an asset. The copyright on that book is the property. The author can, and usually does, sell the property to a publisher, thus selling off the right to distribute his or her own work.

Let's see how copyright fits our criteria for a good property system, ranking each criterion from 1 (worst) to 10 (best):

- It gives proportional title over a real investment: 4
- It has explicit and unambiguous boundaries: 9
- It is cheap or free to acquire the title: 1
- It is cheap or free to enforce: 6
- It does not conflict with other assets or property systems: 4
- It has a low or negative cost to the rest of society: 2

The overall score is 35 out of 60. It's not bad, not great. Copyright has some major issues. It is not proportional, lasting far too long. To enforce copyright against a determined cheat, you still need to hire a

lawyer. It conflicts with digital society's social networks, which depend on sharing. Even a marginal amount of copyrighted work in a collection of culture makes the entire culture dangerous to share. The cost to society is high, as distributors can keep prices for works much higher than the real cost of distribution.

Copyright law is based on the theory that reducing cultural sharing is good for society, because the distribution monopoly encourages creators to create. It's a logical theory if you are a certain kind of person.

At best, we can claim that copyright motivates distributors to actively seek out and develop talent that would otherwise wander, feeble and unknown, in the wide world. It provides distributors with an assurance of profit, so they can pay musicians, artists, movie stars, and directors for their work. The outcome seems to be, however, that artists either die from drug overdoses at 28, or live in near starvation, cursing the labels. A cynic might claim that both these extremes produce interesting art. I suspect most creative people would prefer something in the middle.

The Netherlands used to maintain a policy[151] of allowing people to register as official artists. They got a stipend, in return for producing three creative works each month. Paintings, sketches, sculptures, Found Art, anything material. When the government ran out of warehouse space to store the millions of pieces of...trash, they finally came to their senses and canceled the program.

You cannot market-force the creative processes any more than you can market-force a child to dance to music.

A Replacement for Copyright

In recent years, creating and distributing works has become so cheap that the traditional concept of copyright no longer suits. Publishers need no protection from cheats because their investments are close to zero. Indeed, sane publishers realize that the greatest threat

151 https://en.wikipedia.org/wiki/Artist_subsidy_(Netherlands)

isn't people redistributing copyrighted works, it is the public ignoring them.

Speaking as an author, I'd argue that creators do need some protection from cheats; that is, people who copy their work and claim it as their own or mix it into proprietary work. As a creative person, your only asset is your reputation. When people pass off imitations as authentic, that is damaging. Yet as modern digital creators, we absolutely depend on people sharing our content, remixing it, adapting and improving it. Otherwise, we starve.

Can we fix copyright law? Let me try. Consider that the asset is the work itself, that sharing is essential to digital culture, and indeed it's the only way to create a real hit. The 2012 hit "Gangnam Style" was memorable to me for two reasons. One, I was in Gangnam (a district in Seoul, South Korea) when the song came out. Two, it was the subject of innumerable imitators, literally thousands of people making their own remixes with the same music on top of their own video, or their own music and video. The song was a massive success and propelled its singer, Psy, to global fame and fortune.

The YouTube remixes and the record label's wise though unusual policy of allowing them were the keys to Psy's fame. Most labels would have hit remixes with Digital Millennium Copyright Act (DMCA) violations to take them down. Still, one thing the label did not tolerate was people re-hosting the same video. There was one original, clearly labeled, and a thousand imitators doing the marketing.

This is the model I propose. Let's call it "Creative Title," or CT:

- Automatic CT on any digital work, identified by content, a unique title, and author.
- Clear attribution by the hosting site (YouTube, for instance).
- Automatic removal of any identical copies, or copies claiming the same title or author.
- Guaranteed right to remix any work as long as a different title is used.

- No expiration on CT; it can last forever, as long as the user account exists.

That's it. The whole thing can be implemented by content hosting sites without any state intervention — no courts, or lawyers, or police. The main problem is that it could conflict with existing copyright. That can be solved by mandating up-front that all work put into the domain must be correctly licensed.

We can do this for any digital work: text, music, images, video, software. We can do this today by using a mix of a share-alike license (like the Creative Commons Share-Alike license, or the GPL) and traditional trademark. This is what we do in the ZeroMQ communities for the software we make. However, with the backing of content hosting sites, we could dispense with trademarks.

Let's see how this would work in practice. A studio makes a new movie. They upload it to YouTube (obviously, because how else would they distribute it?) on the official studio channel. People immediately make their own versions with fake soundtracks, remixes with other movies, and so on. It's all tolerated, even encouraged, as long as they don't use the same title. The movie goes viral and gets a billion views. The advertising and referrals earn the studio $100 million. Their channel sells toys, gadgets, and other merchandise, which earns them several times more.

Or, I upload a new software project to GitHub. Someone forks that and makes a patch. I merge their patch back into my work. They publish their project under my title, and it gets taken down. They republish it under a new title, and it remains there. All this was possible without any need to define a license, argue about ownership, or worry about mixing proprietary code into an open source project.

It is in fact easy to fix property systems when you realize what they should be doing. The hard part is fixing a system when every justification is a partial or total lie. "Without life-plus-70-years copyright, there would be no incentive to create" is a lie, and debating copyright

terms (Is 50 better than 70? Why not 5, or 1,000?) just reinforces the lie.

Instead, to fix a property system, look at the real assets and investments of society at large, and then look at the cheats and how they work. Then make it as cheap and automatic as technology allows to protect assets and investments from cheats. More often than not, the cheats are individuals or companies who look to capture investments made by wider society.

Speaking of cheaters and their lies, and capturing the work of many for the benefit of a few, let's look at the patent system, a glorious example of a property system done wrong. (Not "gone wrong," since it is working essentially as it was designed in the mid-nineteenth century, making lawyers and cartels wealthy by taxing wider society to use essential technologies.)

Patents

How Good is Patent Law?

There are towns in Texas where the police may follow you[152] if you are an out-of-state driver, black, or Latino. They may stop you on the pretext of driving too close to the white line, staying too long in the left lane, or other imagined offenses. They will ask to search your car, and then claim to smell marijuana. If they find money, jewelry, or even an iPhone they like, they will seize it and possibly your car, too.

They will tell you, "We are seizing your property since we believe it is being used for a crime." Then, they will tell you, "We will also file felony charges against you." If you are traveling with young children or babies, they will tell you, "We will also seize your children and hand them to Child Protective Services." However, if you sign a forfeiture and hand over your valuables, you will be free to leave. Whether you are actually charged with a crime or not makes no difference.

152 http://www.newyorker.com/reporting/2013/08/12/130812fa_fact_stillman?currentPage=all?mobify=0&intcid=full-site-mobile&mobify=0

The State files a civil lawsuit against your property; if you want to fight that, you must pay your own legal costs.

Some police departments get 40% or more of their funding from civil forfeiture. In some states, profits sometimes go to charities and then the abuses are not so marked. Often the profits are spent on the police themselves, including bonuses for officers involved. It is a form of legalized piracy — highway robbery by the powerful on the weak — using the cloak of the State.

The patent system is somewhat like this, though worse. Let's back up for a second and see how patent law scores on our ranking system. It gives disproportionate title over paper-thin investments; it has fuzzy and even cryptic boundaries; it is expensive to acquire; it is expensive to enforce; it conflicts with other assets and property systems to an absurd degree; and it has a high cost to society. I give it a score of 2 out of 60, and that's only because my scoring system doesn't do negatives.

Let me back up further and explain what a patent actually is. It is the exclusive right to use some idea or knowledge (also known as the "invention") in products and services. The patent system deifies the "inventor" and the "invention." The patent has a list of claims, which describe the specific uses of the idea that the claimant wants to own. Patents are checked by examiners, who reject or grant them. Examiners tend to assume that a bad patent will be caught by the courts. The patent is then used to threaten businesses into paying license fees, exiting the market, or accepting other settlements. Patents are judged by specialized patent courts (in the US and soon in Europe), which tend to assume that an examined patent is valid until proven otherwise.

Patents have a long and contentious history. Very roughly, they got their modern form around 1850 to 1870, first being abolished and then reinstituted in Western industrial countries. The main arguments for patents were, and are: they protect long and arduous investments from copycats; they encourage investment in new products; they

stimulate research and development; they protect small innovators from large predator firms; they are a fair and natural reward to inventors; they are a reward for disclosure of inventions; and they are a reward for documentation of knowledge.

None of these arguments stand up to real scrutiny, nor does empirical data back them up. The largest holder of software patents is IBM. Do you know of a single successful software product they have ever made using their patents? The largest and most successful software system ever built was the Internet. Not a single of its protocols is patented.

The patent industry tells so many lies that it's hard to pull them apart. The core lie is that mythological inventor. As I argued in "Spheres of Light", we don't invent solutions so much as discover them, and it takes a society to do this, not individuals. The basic tenet of a patent — namely that a single person or company can create knowledge — is false. Even in the temples of research, such as pharmaceutics or genetics, it's a clear fact: researchers work by sharing knowledge, not hoarding it. The Human Genome Project[153] beat privately funded research in a race to publish sequences before the commercial teams could patent them.

As with copyright and culture, the only way a society can improve its technology is to share and remix. It does not matter how much you bribe your researchers. If they are cannot share, they cannot innovate. Have you seen the latest smartphones from North Korea?

Products and markets and other people are how we test that some knowledge is valid. We don't use some magical process of "invention." Patents claim that discovery by the market does not exist, and if it does, it is piracy.

The lies go much further. A patent is only as good as the innocent infringers it can catch. Patent attorneys write patents to be as vague as

153 https://en.wikipedia.org/wiki/Human_Genome_Project

possible, inventing new language for old concepts, and using any other tricks that make it hard for businesses to avoid infringing.

In a 2013 patent case over diaper elastics[154], one of the judges wrote, "...it appears that claims are drafted with a degree of indefiniteness so as to leave room to later argue for a broad interpretation designed to capture later-developed competition." The extremely fuzzy boundaries of a patent mean that litigation is common and expensive. Just because you license patent A does not mean you are safe from patent B. A common technology like video encoding may have hundreds of overlapping patents.

Patents are expensive to buy and expensive to enforce. To write and file a patent application costs around $10,000 to 20,000. To defend it against low-level challenges can cost half a million. To defend it against major challenges, tens of millions. This makes patents a game for the rich. Small product-making firms that try to use patents tend to find themselves in hot water. Acquiring a patent is like painting a large target on your back. If the patent is worth anything, you can expect to be sued into handing it over.

And each "successful" patent, that pinnacle of a strong personal property right, comes at great cost to society. The Australian CSIRO research institute acquired four weak patents on WiFi and extracted $430 million[155] from the electronics market. Everyone in the industry knows that CSIRO's patents covered existing technology. However, the patents covered a widely used wireless standard with many sitting ducks in its territory.

The first lawsuit hit a small Japanese wireless company, Buffalo. CSIRO filed their case in a patent-friendly Texas court. The judge rapidly ruled against Buffalo, and issued an injunction to ban their products from the market. Buffalo settled, and the industry followed.

---

154 http://www.patentlyo.com/patent/2013/08/judge-plager-construe-ambiguous-terms-against-the-drafter.html

155 http://arstechnica.com/tech-policy/2012/04/how-the-aussie-government-invented-wifi-and-sued-its-way-to-430-million/

CSIRO doesn't make products. Nor do any of the other 10 or so firms claiming patents on the 802.11 WiFi standard. The end result is that firms like Buffalo that are doing real innovation are taxed by private interests who make no products and do no innovation at all.

In the worst cases, where patents hit a really crucial area of technology, cost gravity slows down for two decades while the monopoly owner tries to bully the industry into licensing deals. It happens over and over, from steam engines to touch screens. Patent holders and their wealth offer such a powerful example of the "success of strong private property rights," and the costs remain hidden. Who is measuring expected cost gravity, and raising the alarm bells when it doesn't happen?

Answering the Pro-Patent Arguments

Now let's give the pro-patent arguments a fair and open trial before we take them out back and shoot them. You will often hear these arguments from people who deliberately or credulously support the patent system.

They protect long and arduous investments from copycats.

I already explained why patents don't protect real investment from copycats, and rather, interfere with a free market in knowledge. In terms of economic theory, patents are as solid as blowing up bridges and highways to stimulate local markets.

They encourage investment in new products.

Businesses sometimes claim that without patents, they would not invest. This is trivially falsified by markets such as fashion and food that have no such protection and yet massive production. The first to market wins. Firms that patent heavily tend to stop making products. Monopolies do not build wealth.

They stimulate research and development.

Research institutes such as CSIRO claim that patents encourage R&D. Innovation comes from many small steps and many participants — not research institutes, which I believe are largely bogus

constructions that pander to the egos of academics and politicians. CSIRO's windfall paid for nice cars, higher salaries, and first-class fights.

They protect small innovators from large firms.

This is only true if the small patent holder is a troll, like CSIRO. If it is a product-making firm like Buffalo, holding patents makes it a target for aggressive lawsuits designed to prise out the patent. If you make products, you most likely infringe on other patents.

They are a fair and natural reward to inventors.

There is no such thing as individual inventors. For sure, people discover solutions, yet that discovery happens on a wide front. Patents are assigned to specialists in patent law who happen to have staked first claim.

They are a reward for disclosure of inventions.

Knowledge that could be kept secret or never discovered by others would not be patented. By necessity, a patent covers knowledge that others already have, or will discover. Patenting encourages secrecy and hoarding, not disclosure.

They are a reward for documentation of knowledge.

You could simply pay people to document knowledge. A 20-year monopoly on some knowledge simply because you wrote it down on paper seems disproportionate. Wikipedia is an example of a much cheaper way to collect knowledge.

Costs to Society of Patents

Patent law has high costs to society. What is the cost of 20 years' slowdown of research into solar energy? What is the cost to the market of extracting $430 million in private taxes in an area — communications — that is utterly essential to the progress, if not the very survival, of our species? More than that, it is a corrupt form of property that encourages a psychopathic "might makes right" view of the market where private profit is always good, no matter the cost to wider so-

ciety. It drives wealth from the many to the few, and creates concentrations of power that corrupt.

Michele Boldrin and David K. Levine, in "Against Intellectual Monopoly"[156], write acidly:

> *A realistic view of intellectual monopoly is that it is a disease rather than a cure. It arises not from a principled effort to increase innovation, but from an evil combination of medieval institutions — guilds, royal licenses, trade restrictions — and the rent-seeking behavior of would be monopolists seeking to fatten their purse at the expense of public prosperity.*
>
> *This cancer is attacking the most vital centers of our economy: metastasis is near and so it is time to face the intellectual monopoly threat squarely, and to take action.*

CSIRO's patents (Thank you, US Patent and Trademark Office!) turned it from a place to stick semi-retired academics into a gangster outfit. Its "success" will modify Australian policy in favor of stronger patent laws and more investment in banditry. The decent, productive sectors of Australian society will have to fly economy class, lose political support, and find themselves taxed by the gangsters.

More than that, the attorneys who made this happen will get jobs in the Australian patent office. They will be the ones defining state patent policy. They will lobby for expanded scope of patents, enforcement of patents on trading partners in Asia, unification of the US and Australian patent systems, and so on. When they have completed a few years in that role, they will find themselves hired as top patent advisors by large firms. This is how the patent establishment has grown and survived over the last century: by pouring money into policy and then reaping a hundred times back from the market. This "revolving door" is a core mechanism of the patent industry.

Private property has such sacred power that patents can easily trump competition law. Creating a cartel to fix prices is highly illegal.

156 http://levine.sscnet.ucla.edu/general/intellectual/against.htm

If the milk producers tried that, they would go to jail. When the phone companies agree to license key patents thereby excluding competitors, the antitrust regulator can do nothing. Patents are the only reason, when I drive across the border from Belgium to France or the Netherlands, I pay EUR 3.50 per megabyte of mobile data versus EUR 30 for my "2.0 GB + unlimited phone calls" plan.

A Replacement for Patents

The patent system has no function other than to enable gangsters dressed in suits to call themselves "honest businessmen." There seem to be a lot of bandits in power around the world, so it's highly unlikely that our current crop of leaders would see the patent system as "bad." Sure, it steals from the poor to give to the rich — what's the problem with that?

A replacement for patents should focus on the investment in products and the knowledge accumulated by small firms. Instead of allowing monopolies, a better system would make them illegal by mandating that:

- Any product sold on the market must have a published bill of parts or ingredients.
- All industrial processes must be documented and that documentation made freely available.
- The right to leak processes and parts for commercial products would be protected by the State.
- The right to copy and modify a product would be protected by the State.
- Product titles and names would be protected by a simpler form of trademark.

I'm not describing a dystopia or theoretical world. This is effectively how the fashion industry and open source software industry work. I think the same models would scale well. Of course the patent lawyers and cartels would fight such reforms to the death.

Assets and Property in the Digital Economy

Stepping carefully around copyright and patents, let's look at the other assets, possessions, and properties that comprise the digital economy, from most tangible to least obvious.

Content

The most tangible assets on the Internet are its content: text, photographs, videos, software, and music. Never in history has there been so much culture available so widely. It has immense value that is very hard to measure.

The usual way to measure the value of something is to measure its cost. For instance, in 2008 the project at the heart of the Linux operating system, its kernel, was valued at $1.4 billion[157], about 10 times the cost of Microsoft's Windows NT. The cost of a full Linux distribution (like Android) came in at over $10 billion. The value of Linux (rather than its cost) is arguably tens to hundreds of dollars per device, and there are half a billion devices running Android alone. I'd suggest that Linux is worth 50 to 100 billion dollars.

Domain Names

A domain name translates a printable name into a real Internet address. Domain names are cheap to acquire and enforce, and clean containers for the asset represented by a website, its content, and community. The cost to society is negligible.

Whether domain names are property or not is arguable, and courts do not all agree. The patent and copyright mafia is keen to bring domain names into their "intellectual property" stable. Other people argue that domain names are just a contractual agreement for a period of time to have a name like "hintjens.com" translated to some physical Internet address. However, domain names have clear boundaries, can be traded, and grant exclusive rights over the asset (the website). They

157 http://www.linuxfoundation.org/news-media/announcements/2008/10/linux-foundation-publishes-study-estimating-value-linux

may not be a de jure property right in all jurisdictions, yet they are property by my definition.

Domain names do conflict with trademarks. These conflicts are mostly rapidly resolved by various dispute resolution mechanisms. Trademarks usually trump domain names.

There is also a problem with people registering domain names that protect non-existent assets, in speculation of their own or others' future investments. This means that many potentially useful domain names are registered and never used, which is a loss to society.

The temporary nature of domains creates wasteful entropy, as references become broken, leading to "link rot." For example, in the FFII we started many projects with their own domains. As people stopped paying for those domains, the project websites became unavailable. This is not good for archival purposes.

Finally, the domain name system grants private interests monopoly control over top-level domains (.com, for instance). The rationale for this was to push the costs of domain name management to business, though the outcome has been a new private tax on the digital economy.

Fixing the domain name system is pretty simple. We already have an international organization, the Internet Corporation for Assigned Names and Numbers (ICANN), that routes the root servers and contracts out to registrars who run each top-level domain. ICANN should cancel all deals with registrars, creating a single domain marketplace, and remove the concept of private top-level domain by allowing anyone to register any domain with two or more levels. Domain names should be free and should last forever. Non-use of a domain (or abuse for purposes such as link farming) should be grounds for losing it.

Trademarks

Trademarks are mostly harmless. They are well bounded, so accidental infringement is difficult. There do exist trademark trolls,

though they are rare. Trademarks are cheap in historical terms and reasonably easy to enforce. In digital society, domain names serve the same purpose as trademarks, and do it better. Why should I trademark "IMATIX" when I own imatix.com?

I'd fix the trademark system by merging it with domain names, so that a trademark is an additional right you can buy on top of a domain name. For instance, if I can show that I've used a business or product name for some time, I can ask that all domains containing that word be protected. That stops cheats from using my business goodwill for their own benefit. Since this is a large exclusion, it should — like a trademark is now — not be too cheap. This would also fix the current conflict between trademarks and domain names.

Standards and Protocols

A standard is a curious thing. It is a form of property owned by a group, created by consensus, and its main purpose is to define a competitive market that will encourage buyers and sellers to invest. For example, we have standards for electric power sockets. That lets us invest in putting electricity into homes and offices, and buying equipment that will use it. If every provider had a different voltage, we wouldn't invest as much in fridges and washing machines.

Let me explain very briefly how standards work. You might think it's all about making revolutionary new concepts available to the public. In fact, standards are more about stopping innovation than opening the door to it. Standardization always works from the bottom up, from more basic and broadly used technologies to more sophisticated and narrowly used ones. Over time, the stack of standards gets compressed like seams of sediment and unused stacks fall away, leaving fewer and fewer basic standards underpinning the whole world of computing.

The economic basis for making standards is the concept of "natural monopoly." This means — at least in this context — that a successful standard will attract and hold all users. Currency is an example: when

the State decrees a particular currency to be legal tender, this becomes a natural monopoly. Holding other currencies means you can't trade, except at a penalty. Similar natural monopolies are rail transport, electricity, phones, and the Internet Protocol. You want your toaster to plug into any power socket. You want your phone to reach anyone and be reachable by anyone.

When a successful natural monopoly emerges thanks to luck, regulation, or market forces, it eliminates a lot of waste — also called "friction costs," "transaction costs," or perhaps "excess profits." Natural monopolies can create huge value. Vendors (those selling stuff) have a corresponding incentive to try to capture that value, restoring profits that would be lost by too much of Adam Smith's invisible hand. The natural monopoly can benefit users by releasing value. A good example: the Internet. It can also punish them by capturing users and then taxing them without mercy. Your mobile phone bill is a case in point.

The dream of every self-respecting patent troll is to get patents on a widely used standard, CSIRO-style. Owning a standard allows the owners — usually a consortium of firms, often including patent trolls — decide who gets to implement it. This is how large firms keep control of the audio and video encoding markets, the mobile phone market, WiFi, and so on. Consortium standards are generally backed up with patents (because it's a far easier argument to the regulator to say, "We're licensing our patents under a Fair! and Reasonable! and Non-Discriminatory! basis" than "We're a cartel of crooks, and we'd like to offer you a consultancy gig."

The most potent and profitable standards are those that are not captured by any business. The Web is built on Requests for Comments (RFCs) that are open to all. Open standards create new markets. Closed standards extract rents from existing markets. Many firms forget or ignore this lesson, and aim to define standards as tools to control markets rather than create them. Standards for mobile phones, streaming music, video encoding, and so on, appear success-

ful, yet they are all dead ends and survive only thanks to the patent system.

The RFCs, a collection of thousands of open standards, are an immense asset. They are also brutally effective. In the decade before 2010, Microsoft especially spent a lot of money trying to hijack existing standards with patents, get its patents into new standards, or force its patented standards into government use. Digital society spent a lot of effort fighting back.

One of my projects, launched in response to Microsoft's hijacking of the EU's open standards process in 2007, was the Digital Standards Organization[158] (Digistan), which built a set of templates for small teams to develop standards cheaply. It used the GPL as license to stop cheats (people modifying the standard to make closed versions).

In my work for the ZeroMQ community, I write a lot of standards and protocols[159], and all these use the Digistan templates. It works very well, and is extremely cheap. The only flies in the ointment (imagine a swarm of flies the size of horses, spitting nuclear poison out of multiple heads) are patents.

Licenses

A license is a grant to use a specified property under specified conditions. Licenses govern most content on the Internet. Without a license, only the copyright holder can redistribute a work. There are many licenses of different types. Many represent huge investments of legal time and expertise. The largest open communities depend on one or another kind of license that allows sharing of different kinds.

Non-trivial licenses are themselves governed by copyright. This means that you cannot, for example, make remixes of them without permission. That is ironic in the case of licenses like the GPL.

As property, licenses work very well. They have no cost, clean boundaries, and are relatively easy to enforce by using the threat of

158 http://www.digistan.org

159 http://rfc.zeromq.org/

copyright action. However the very existence of licenses and the need to use them signal a problem. Many people do not accurately license their work because they forget.

If Creative Title (TM) replaced copyright, content licenses would be unnecessary and could be scrapped.

Identities

How much is your email address worth to you? Email addresses and user profiles are de facto property, protected by the courts in some ways. Boundaries are clear and enforcement is simple: don't lose your password or allow a virus to run on your computer.

God help you if someone steals your identity on a large site, though. You will not find a person in technical support to help you, in a hundred years. While there is legal protection for privacy — stealing someone's emails is a criminal offense — there are no laws to protect your identity on the Web. This is a problem because our identities are one of our biggest investments and assets.

I propose an identity protection system based on who we are and where we go, and one that is not really private: a central registry, perhaps maintained like domain names by ICANN, where you can register a name and profile. This would be used to sign in to participating websites with different passwords for each website. Systems like this already exist to some extent, such as OpenID[160].

On-line Games

The most incomprehensible of assets (to an outsider) are those used in on-line games. Monopoly money, so to speak. Most games start and stop, yet the "massively multiplayer on-line role-playing games" (MMORPGs) continue forever. This means players can, and do, accumulate assets over time and build realistic simulations of property, economies, and currencies.

160 http://openid.net

These virtual economies are interesting in how they develop. Each game is, in effect, a state with its own rules and authority. There is a large secondary market, probably around $1 billion a year globally, for game assets such as avatars and in-game currencies. When the operators of a game regulate the market and economies, they create black markets.

Linden Labs launched the Second Life[161] game in 2003, and had about 600,000 active users by its tenth anniversary. Its currency, the Linden dollar, is convertible to "real" currencies via market-based exchanges. This means Linden Labs had to regulate its virtual society and economy quite carefully, not always to the delight of users whose in-game businesses suddenly became illegal and were stopped.

One of the more interesting games, *EVE Online*, prohibits the conversion of in-game currency or items into real money. This means in-game fraud, banking, theft, gambling, murder, and the destruction of masses of virtual property can be allowed. The result is a more interesting game. The big battles in EVE Online involve thousands of players and ships[162], and destruction of property worth tens of thousands of real US dollars. From Wikipedia's article on EVE Online[163]:

> *One infamous example was an infiltration and heist where one corporation infiltrated a target corporation over the course of nearly a year. They then performed a virtual assassination on the target's CEO and proceeded to steal corporate property to which they had gained access. The target corporation lost billions of ISK worth of property (amounting to about $16,500) and a great deal of prestige; the CEO's expensive ship and cybernetic implants were destroyed in the attack.*

The existence of black markets for on-line gaming communities reveals the problem with non-convertible assets. I'm not sure what the

161 https://en.wikipedia.org/wiki/Second_Life

162 http://www.theverge.com/2013/7/28/4565558/eve-online-biggest-space-battle-in-history

163 https://en.wikipedia.org/wiki/EVE_Online

solution is, though I think it involves more freedom to convert in-game assets to and from real currencies, without risk of lawsuits or prosecution.

Communities

Some of the most valuable, and least tangible, assets of the digital economy are its communities. You might think a community is owned by the company that runs the website and owns the domain name, and you would be wrong. The community aspires to own itself, and be highly mobile.

This is the lesson we learned from the MySpace story. A poor authority will see its assets flow away, not quite overnight, yet within a few years, perhaps even months. When Oracle bought Sun in 2010[164], they also took over Sun's many free software projects, including MySQL and OpenOffice. Within a few months, these had forked — as allowed by their open source licenses — to create MariaDB and LibreOffice, simply because Oracle was doing what it does best, being arrogant and overbearing. That works well with corporate clients. It is not the ideal way to treat on-line communities.

Industrial-age businesses survived by capturing their clients. Digital-age businesses survive by bribing their clients with freedom and getting them to co-invest in their properties. Look at how Amazon entices its clients to become partners. Review this book and become part of our marketing machine. Your opinion matters! It's mutually profitable and it's honest.

When a firm owns the domain name and website for an on-line community, it owns the *anchor* for the community. This makes it the authority, able to define licenses, rules, and policies. If it is a good authority, the community will stay there and grow. If it is a poor authority, the community will fragment, detach, and move to another anchor. Who owns your Twitter profile? You do, of course. Who enforces that property? Twitter does.

---

164 https://en.wikipedia.org/wiki/Sun_acquisition_by_Oracle

So digital society is filled with authorities, from huge ones like Google, Facebook, and Twitter, with hundreds of millions of citizens, to tiny ones with a handful of participants. Me, myself, and I make three. These digital authorities define their own property laws, and enforce them without negotiation, and are thus analogous to a State. Such digital authorities are the digital successors to the industrial-age nation-state.

Digital society is not a single authority, it is many. When an authority tries to cheat, the outcome is simple: people abandon it. The freedom to leave one on-line community and go to another is unquestioned and unparalleled in the real world.

Knowledge

Finally, we have the intangible asset called "knowledge." Of all the websites in the world, one is precious beyond any measure, and becoming more so every day, and that is Wikipedia. Any attempt to describe how important and valuable Wikipedia is would fail by understatement. As a species, we only really have two fundamental assets: ourselves, and our knowledge.

When I scored Wikipedia in "Spheres of Light", it hit 96%. Wikipedia is not perfect, though it comes close. This isn't accidental — it was practically founded on the principles of the wisdom of crowds. The one area it does not handle perfectly is current events — politics, sports, news — where there is still money at stake.

Wikipedia is the ultimate in collective property, the antithesis of private property with its strong rights, de jure protection, profits, and friction. It is the ultimate slap in the face to the right-wing economists and their belief that wealth comes from individuals rather than society. I relish my personal possessions as much as anyone, yet the collective property that is Wikipedia's knowledge stirs deep joy in me akin to religious fervor.

Money in the Digital Economy

The industrial economy had a very clear definition of money: legal tender, issued and regulated by the State. Currency was coin of the realm, and the realm could make it, or break it.

Often, the world had a "reserve currency" that was considered the most stable and convertible, and held by governments as part of their foreign exchange reserves. For a long time, this was the British Pound Sterling. Then in the middle of the last century, the US Dollar became a significant reserve currency, and at the start of this century, the Euro joined. The government behind a reserve currency tends to use it to create debt, which then causes the currency to deflate and the world to switch to another. This seems to be happening with the US Dollar today, though it's unclear what the future reserve currency would be.

The Internet has been searching for a reserve currency, indeed any currency that could be used to buy goods and services on line, for a long time. The digital economy presents a unique set of challenges for security and privacy.

Credit Cards

Most Internet trade still uses credit cards from firms like Visa and MasterCard. These firms charge merchants about 3-4% on each transaction, which is an astonishing amount and points to a cartel operation. Indeed, these two firms have been under fire from European antitrust authorities for years. They should have gotten some patents.

Mobile phones can now be turned into wireless credit card terminals by using little credit card readers that plug into the phone. The customer swipes their card to make a payment. It is all rather impressive, until you realize the deceit. The currency is all digital, held in bank accounts somewhere. The devices are all digital. The credit card itself and that little reader are a physical bridge between a digital financial system and itself.

Credit cards are a very bad fit for the on-line economy. To make a transaction, the buyer gives his credit card details to the seller, who re-

gisters the transaction to the credit card company, which then authorizes it. The buyer only sees the details at the end of the month, and the seller may have to wait for several months to receive his money in his "merchant account" minus the processing fees and any disputed transactions ("chargebacks").

It takes a decent credit history to qualify for a "merchant account." This puts credit cards out of reach for newer, smaller sellers. Thus a second layer of businesses have cropped up which offer credit card processing to websites, adding further costs and delays on top.

Exchanging credit card details across insecure networks to strangers is an invitation to fraud. By 2000 or so, to use a credit card on the Internet was akin to driving without a seatbelt on the wrong side of the road.

PayPal: the Web's Bank

The need for safe transactions between strangers was nowhere more obvious than on the eBay auction site. In 2000, two existing financial service firms (Confinity and X.com), which already allowed users to email each other money, merged to form PayPal. Their successful strategy was to focus explicitly on eBay users in the US, then grow internationally.

PayPal did a decent job of building a payments system that worked for on-line commerce. Though credit cards are widely used for purchases, sellers will often use PayPal as their payments processor. PayPal is cheaper and easier than the credit card companies and takes only 2% instead of 4%, allowing anyone to become a merchant.

However, PayPal built a reputation for being a bit of a thug. It tended to seize accounts without explanation, freeze payments to sites without explanation, and even cut off entire countries[165]. Its customer service is legendarily bad. Many websites simply refused to work with PayPal at all.

---

165 http://java.dzone.com/dose/dzone-daily-dose-210

eBay bought PayPal in 2002, and despite its poor reputation, the service grew into what is today one of the largest web payment processors. It is, in effect, the Web's bank — hated by many, yet a fact of life. In Europe, PayPal is in fact regulated as a bank, while in the US it is licensed as a money transmitter, which is a key license. The PATRIOT Act makes it illegal to transmit funds from account to account without such a license. The loss of this license would effectively kill PayPal.

Micropayment Systems

As the Web boomed from 1995 to 1999, various groups developed micropayment systems that solved credit cards' high transaction costs. The theory at that time was that people would, for example, pay a few cents to read an on-line newspaper.

These systems were developed, cast into official standards (the HTTP web protocol has an error code called "Payment Required"), and then quietly abandoned due to lack of interest. It turned out that advertising worked much better as a micropayment system, which brought us Google. Advertisers pay the website operator via Google each time a visitor clicks on their advertisement.

The massive volumes of free content also hurt the case for micropayments. There are a few businesses[166] that use so-called "paywalls" successfully. Typically, these are existing publishers whose subscribers already expect to pay. The focus however is on subscriptions, not micropayments.

In 2002, the M-Pesa[167] system formalized mobile phone micropayments in Kenya. Before that, users sent each other phone credit. Phone credit makes an extraordinarily good digital currency, as it is safe, portable, and has minimal transaction costs. Systems like M-Pesa succeeded in Africa mainly because there was no existing financial in-

166 http://www.cjr.org/the_audit/the_nyts_150_million-a-year_pa.php

167 https://en.wikipedia.org/wiki/M-Pesa

dustry to lobby against it. Good luck trying to get a Visa card if you live in Lagos, Nigeria.

Digital Currencies: From E-Gold to BitCoin

The first digital currency was e-gold[168], founded in 1996. At its peak, e-gold had five million users and transactions of $2 billion a year. An e-gold account was backed by actual gold held by the service. One e-gold account could then transfer gold to another account. The company offered interfaces to allow websites to accept payments in e-gold, much like PayPal did later.

e-gold died in 2009 after a long struggle with fraudsters, imitators, and patent lawsuits. It was finally killed by the US federal government, which first denied it the all-important money transmitter's license, and then prosecuted it under the PATRIOT Act for transmitting money without a license.

It is safe to assume that e-gold was deliberately targeted, not because it allowed terrorists to collect money (US dollars work much better for that), rather, because it was a viable digital currency. The use of anti-money-laundering regulations and the PATRIOT Act to attack a digital currency is, I'd claim, a good indicator of how seriously the currency threatens to succeed.

The same year that e-gold died, its successor popped up in the form of BitCoin, the first credible crypto-currency. While e-gold based its denomination on the tangible value of gold coins, BitCoin is backed by nothing more than mathematics. This has led people to accuse it of being a pyramid scheme, destined for collapse.

BitCoin works by "mining" new coins as a side effect of doing the cryptographic bookkeeping for other people, processing the so-called "transaction chains." In the beginning, when transaction chains were short, they were easy to process, and people could mine thousands of coins on their PCs. Today, as chains are long, it takes more effort to

168 https://en.wikipedia.org/wiki/E-gold

mine coins. Every year, the number of coins that can be mined falls, so at some point there will be no new BitCoins.

The BitCoin design and open source software was written by a prudently anonymous team calling themselves "Satoshi Nakamoto." They took some existing concepts from the cryptographic community, and invented some new ones. The technology had one major vulnerability, which was fixed in 2010. Since then, it appears robust.

BitCoin satisfies most of the criteria for use as a medium of digital trade. It is free from coercion by authorities. The transaction fees are paid in the form of computing power used to verify blocks and network bandwidth to exchange chains with others. It allows micropayments.

There are some vulnerabilities with BitCoin:

- As a small currency, it is still vulnerable to speculators and exchange rate attacks. Its value has often been very volatile.
- To convert to and from other currencies, BitCoin depends on exchanges, which can be attacked.
- It is unclear whether people will still go through the effort doing block verification when no more BitCoins can be mined to pay for the work.
- If a large attacker were to control more than half of the verification network, they could generate unlimited BitCoins and destroy the currency by inflation.
- It depends on conventional broadband, so is vulnerable to surveillance. BitCoin transactions are public and individual BitCoin holders' transactions can be identified.
- It depends on a "digital wallet" held on a computer, which is vulnerable to malware attacks and physical seizure.

The history of money on the Internet and the power of the banking industry suggest that BitCoin will come under serious attack in coming years. We can expect to see the same attacks that we've seen often before:

- Financial blockades, prosecutions, and technical attacks on BitCoin exchanges.
- Association of BitCoin users with terrorists and child pornographers.
- Surveillance of BitCoin transactions to break expectations of anonymity.
- Interference in the BitCoin verification network.

As an exercise, I tried to buy some BitCoins. Since I don't know anyone with BitCoins to sell, I looked for an exchange with coverage for Europe. A bit of searching led me to a European exchange, Bitstamp.net, where I registered and prepared to make a small deposit to the exchange's bank account in Slovakia. My banking website refused to accept the transfer, showing an error that I've never seen before in decades of making international transfers. I tried a few times, then gave up. One imagines an "attempted to buy BitCoin" flag being set on a dossier somewhere in a secret Spider data center.

The New Billionaires

How much is a Facebook "Like" worth?

In 2011-2013, the US State Department spent $630,000 to buy nearly two million likes on Facebook. It's doubtful anyone actually liked the government more afterwards, except the consultants doing the work. It shows the real value we are willing to place on our on-line reputation.

I think we have vastly underestimated the value of the digital economy. I tried to show how many assets it has, yet many — like the content on Wikipedia or YouTube — are considered worthless because they are "free."

Is it possible to calculate the gross Internet product (GIP) to compare to the gross world product (GWP)? We can count the assets created in all the virtual worlds, as it's clear that people clearly assign value to them or else they would not create black markets, nor pay for "Likes."

Let's assume that two billion people regularly toil on line, spending 20 hours a week in constructive work (not just flipping through YouTube channels). The Organisation for Economic Co-operation and Development (OECD) average GDP is $35,000 per capita. Let's assume that the on-line society is as productive as the OECD average. The ratio is probably much more than one because the digital economy is so much larger and more efficient. However, this suggests that our investment in on-line assets is around half of our investment in the real world, which seems to match empirical observations.

This gives us a GIP of $35 trillion a year. When we hit four billion Internet citizens, the GIP will start to exceed the whole industrial economy. (Actually, since GDP includes all Internet transactions, the industrial economy is already smaller than $70 trillion.) I think this estimate is low, and that the real productivity on line is both higher than in the real world, and growing faster than we think. However, I'm not an economist. Perhaps a proper economist will find better figures.

One claim that I am making that you might have missed is that our on-line productivity is not dependent on where we live. That is, a poor person invests just as much as a wealthy person. This means that for poor countries, the digital economy is much more powerful a shift than in wealthy countries.

The peak population of the Internet will be around 10 billion, in 2030, and I'd estimate per capita GIP of $100,000 by then, giving a global GIP of a mind boggling $1,000 trillion (that's a one followed by 15 zeros).

The Price of Salt

My children were amazed to learn that ordinary salt used to be a currency: the origin of "salaries" and "salads." It costs perhaps $1 per kilo in the supermarket, and eight times less if you buy a truckload.

There is a theory of wealth, which is that for every rich person, there must be a poor person. This is indeed how it sometimes seems to happen. However, the theory is wrong. Despite disparities that may be huge, overall society generally gets wealthier together, thanks to cost gravity. The tragic exceptions, like Congo-Kinshasa, where life expectancy has fallen from 55 in the 1950's to under 50 today, underline the general rule that most of the world has gotten wealthier together. Much of that new wealth is invisible to the old economy, yet it has a very important effect on it.

One of the shocking things about American society is its inequality[169]. The bottom 80% of the population own less than 7% of the nation's wealth. Many people are in permanent debt and worth less than zero by traditional measures.

The disproportionate accumulation of wealth by the already wealthy has not caused a revolution — not even mass protests. Basically, people are happy or resigned enough with the way things are. One explanation is that the mass of people are brainwashed, bribed, and blackmailed by what is in effect a nationwide cult system. This is certainly at least partly true. If you ask the average American citizen, "Why aren't you in the streets protesting the unfairness, the spying, the corruption," they probably won't reply, "I'm afraid of being arrested," and will instead say something like, "I don't really see that it's necessary."

I don't think that this is the result of complacency. Rather, I think most people have accurately and subconsciously assessed that old money is like salt. It's still essential, of course. Without salt, you die.

---

169 http://www.pewsocialtrends.org/2013/04/23/a-rise-in-wealth-for-the-wealthy-declines-for-the-lower-93/

Yet only fools fight over salt, and only madmen accumulate cellars of the stuff on the off chance that its price will one day go up again.

The trillions hoarded by the mega-rich cannot buy friends on the Internet. It cannot buy truth on Wikipedia; it cannot buy success in digital markets, bribe the digital authorities, or convert into any real form of power in digital politics. People have tried this over and over and it keeps failing[170].

Conclusions

In this chapter, I've looked at the digital economy and its assets, bouncing off copyrights and patents in the process. I came to the perhaps raving mad conclusion that the gross Internet product (GIP) is already about half the size of the global world product (GWP), the total GDP of all countries on earth. More insanely, I'm claiming that by 2030, when 10 billion people will be spending most of their waking time on line, GIP will be 10 to 15 times today's GWP.

This explosion in assets is both an existential threat to the Para-state, and the answer to its excesses. As I've written, political power comes from economic power. As the digital economy's power exceeds and then eclipses the old "real" money of the Para-state, the political conflicts will increase, alliances will be formed, and we will see the outbreak of a real world-wide conflict, ending in either the death of digital society, or of the Para-state. The war has been going on for some time now, and this is what we'll examine in the next chapter.

170 https://www.google.com/search?q=microsoft's+stock+price

Chapter 7. March of the Kaiju

It's out of conflict that new political structures emerge, for politics is essentially about organizing disparate groups and factions to win power through some kind of conflict, and then keeping these groups in balance to prevent further conflict.

In this chapter, I'm going to look at how that network of agencies I've termed the Spider is consolidating its grip over the world both digital and "real." I'll cover a lot of different areas in this chapter. There have been so many clashes and fights that it is difficult to choose a few to turn into a story. And like any reporter, my choices will expose my own interests as much as anything.

The Death of Politics

When I look at modern politics, I see a surprising thing, a sign that our world has fundamentally changed, and the old rules of politics have been replaced by a new, unspoken set.

I'm no fan of the old left/right divide, which was like being asked to choose between two equally repugnant churches. Nonetheless, one of the memorable features of politics of the past used to be the existential conflict between political parties, which drove real debate, and legislative change. A party either represented its views, or it died.

This is mostly gone. In countries with proportional representation, and many smaller parties, politicians work by consensus, which leads to stagnant, cold-blooded entrenchment of old structures. Much of Europe suffers this. Gerrymandered America suffers the same, though it masks the back room collusions with politics as circus.

In the UK and US, birthplaces of parliamentary politics, real debate died after 2001, as evidenced by the decision of these two countries to invade, with lies and propaganda instead of formal declarations of war, first Afghanistan, and then Iraq. Political debate in both the UK

and US has become a form of reality show, drama for the viewer, without substance or meaning.

The lack of real debate is astonishing, because you would normally expect politicians to take every opportunity to attack each other on policy, to secure their own power. Conflict between factions of politicians is one essential balance of power. If this goes away, we have to ask how that happened.

Let me list a few of the issues where I'd have expected there to be real, angry, excited argument and conflict in Washington and Westminster, instead of passive statements of outrage followed by inaction:

- The financial crisis, and the criminal role of the financial industry in this.
- The war of aggression in Afghanistan and Iraq, with their bogus rationales, serious loss of life, and immense cost.
- The explosion of the security apparatus, with its intrusion on private life, and cost.
- The War on Drugs, with its disastrous effects on many countries hosting the drug trade.
- The revelations about the NSA's snooping on the private communications of pretty much everyone.
- The ongoing detentions in Guantanamo Bay of individuals convicted of no crimes.
- The renditions, tortures, murders, drones, and other violences of the War on Terror.
- The lack of prosecutions for the financial fraud leading up to the 2009 crash.
- The increasing gap between the very rich, and everyone else.

And so on. These issues float around the media, sometimes making headlines, and politicians make vague gestures of concern, yet with little or no real passion. Only outliers seem to take these seriously, and these outliers get no airspace, no visibility except in the underground

alternative media. It is as if the political establishment, along with the mainstream media, has come to undivided silent agreement that none of these issues matter. On the contrary, to the majority of people, that is those nominally electing those politicians, these issues are absolutely vital.

It's not just the lack of fighting inside Congress and the Houses of Parliament that is historically atypical. It's the total suspension of normal political opportunism. When President Clinton was caught with his pants down, the response from the Republican party was ferocious and unrelenting. Yes, absurd, yet that is why we elect psychopaths to power. They are the only people we can count on to stick the knife into the other psychopaths when they see the chance.

And yet, after eight years of arguably the most criminal US regime so far, the Democrats under Barack Obama stuck to empty debate on safe topics, engaged in dramatic theater over budgets and health-care, and then continued much the same policies.

The only thing that will get hundreds of politicians to agree, for years, is a larger bully. As I explained in "Eyes of the Spider", the threat of Global Terrorism is a bogeyman, blown up to a multi-Trillion dollar industry. So-called "international terrorists" are, as I'll explain in "The Reveal", mostly recruited and organized by the Spider itself.

There are no alien invasions. And Washington and London certainly do not yet see the digital revolution as an existential threat. So what is going on? Why the decade-long suspension of the democratic process? *Why are the politicians not fighting?*

I see two plausible answers. One, the US and UK turned mysteriously into socialist Scandinavian heavens of consensus politics. Two, the herds of politicians are being bullied by a larger, nastier predator. I think we can rule out the first option. The predator is, of course, the Spider, built-up by the Para-state as its Praetorian Guard, and like all imperial guards, itchy for the power it sees wielded so poorly every day.

A common response to hypotheses of large-scale plots is "Bah, conspiracy theories! Someone would talk." In fact there have been many whistle blowers who have talked, about large-scale plots of all colors. There is no lack of people who are willing to talk, and often provide very specific, detailed knowledge of crimes committed behind the curtains. The common factor with the whistle blowers is that the mainstream media ignores them unless their stories are pushed through alternative platforms so dramatically that they cannot be ignored. Chelsea née Bradley Manning disclosing crimes through WikiLeaks provides a well-known instance of this.

One of the first significant NSA whistle blowers was Russ Tice[171]. He told us in December 2005 that the NSA and DIA (another three-letter agency I'll come back to in the last chapter were spying on US citizens, something that was, and still is, illegal. The NSA then fired him, and rebuffed his claims. Today, we have corroboration of what he said, from Snowden and indeed from the NSA themselves. On June twentieth 2013, on the Boiling Frogs podcast, Tice went much further[172], saying:

> *[The NSA] went after high ranking military officers. They went after members of congress. The Senate and the House — especially on the intelligence committees, and on the armed services committees and judicial. But they went after other ones too. They went after lawyers and law firms. Heaps of lawyers and law firms. They went after judges.*
>
> *One of the judges is now sitting on the supreme court that I had his wiretap information in my hand. Two are former FISA court judges. They went after state department officials. They went after people in the executive service that were part of the White House — their own people!*

171 https://en.wikipedia.org/wiki/Russ_Tice

172 http://www.boilingfrogspost.com/2013/06/19/podcast-show-112-nsa-whistleblower-goes-on-record-reveals-new-information-names-culprits/

> *They went after anti-war groups. They went after US companies that do international business around the world. They went after US banking firms and financial firms that do international business. They went after NGOs like the Red Cross and people like that that go overseas and do humanitarian work.*
>
> *They went after a few anti-war civil rights groups... This thing is incredible what the NSA has done. They've basically turned themselves — in my opinion — into a rogue agency that has J. Edgar Hoover capabilities on a monstrous scale on steroids.*

Structure defends itself. To be honest I'm surprised Russ Tice still lives. The alphabet agencies defend themselves, and their greatest threat is a cut to their funding, or oversight from politicians. Thus, their absolute first priority, before stopping any terror attacks, must be building up files on any individual with power. The Spider's "persons of interest" are not Chechen rebels, Somali militants, or Syrian fighters. I think the consistent failure to stop real attacks shows that. Their persons of interest are, as Tice says, members of congress, generals, judges, lawyers, journalists.

Tice continued, "One of the papers that I held in my hand was to wiretap a bunch of numbers associated with a 40-something year old wanna-be Senator from Illinois," referring to the future President Barack Obama. Hence the reference to J. Edgar Hoover. As Wikipedia says[173]:

> *According to President Harry S. Truman, Hoover transformed the FBI into his private secret police force; Truman stated that "we want no Gestapo or secret police. FBI is tending in that direction. They are dabbling in sex-life scandals and plain blackmail. J. Edgar Hoover would give his right eye to take over, and all congressmen and senators are afraid of him."*

173 http://en.wikipedia.org/wiki/J._Edgar_Hoover

The focus on politicians seems to reach globally[174]. In June 2013 the Guardian reported that[175],

> *When G20 finance ministers met in London in September, GCHQ again took advantage of the occasion to spy on delegates, identifying the Turkish finance minister, Mehmet Simsek, as a target and listing 15 other junior ministers and officials in his delegation as "possible targets." As with the other G20 spying, there is no suggestion that Simsek and his party were involved in any kind of criminal offence. The document explicitly records a political objective — "to establish Turkey's position on agreements from the April London summit" and their "willingness (or not) to co-operate with the rest of the G20 nations."*

Such spying was for explicitly political objectives, as opposed to terrorism, the standard bogeyman. As we've seen before, the Spider cannot work alone. It needs the help of technology firms of all kinds, to supply the hardware and software, and to provide access to networks and servers. The role of technology firms isn't a secret. Also in June 2013, Bloomberg reported[176] that "Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence, four people familiar with the process said."

And as Bush granted retroactive immunity to the telcos for helping with the NSA's warrantless wiretapping program, Politico.com reported that General Keith Alexander[177], head of the NSA, "has petitioned

---

174 http://www.zerohedge.com/news/2013-06-16/nsa-uk-spied-politicians-intercepted-emails-eavesdropped-russian-presidents-phone-ca

175 http://www.guardian.co.uk/uk/2013/jun/16/gchq-intercepted-communications-g20-summits?CMP=twt_fd

176 http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html

177 http://www.politico.com/story/2013/06/nsa-keith-alexander-cyber-shield-9288

Capitol Hill for months to give Internet service providers and other firms new cover from lawsuits when they rely on government data to thwart emerging cyberthreats." One wonders why firms would need immunity, if they are not breaking any laws.

If the Spider did execute a silent coup against democracy, it started a long time ago. In 1975, following the Watergate scandal, there was enormous pressure from the public, and from congress, on the CIA for more transparency and accountability. The director of the CIA, William Colby seemed open to reforms.

Then, in the so-called "Halloween Massacre"[178] of November 4th, 1975, President Ford fired Colby, as well as many moderate members of his cabinet, and replaced them with hardliners. Three names stand out: George H. W. Bush, who took over as director of the CIA, Donald Rumsfeld, the previous Chief of Staff, who took over as Secretary of Defense, and Dick Cheney, who became Chief of Staff. Bush, Rumsfeld, and Cheney all did well out of that, as did the CIA.

The Insecurity Business

It was strange to picture General Alexander "petitioning" lawmakers like a cheap lobbyist. More than likely, he wasn't really in charge. After all, this was the man who turned his war room into the helm[179] of Captain Kirk's Star Ship Enterprise. One wonders how secure such a person actually felt. We can surmise that although the NSA has the files on every person of interest, it perhaps does not have the real power. I see the NSA as the geeks of the Spider, the CIA and DOD its bullies.

0.html?hp=r1

178 https://en.wikipedia.org/wiki/Halloween_Massacre

179 http://www.theguardian.com/commentisfree/2013/sep/15/nsa-mind-keith-alexander-star-trek

And indeed, after I'd written this, General Alexander resigned[180] "to spend more time with his family." Another nine top generals — Major General Michael Carey, Navy Vice Admiral Tim Giardina, Major General C.M.M. Gurganus, Major General Gregg A. Sturdevant, Brigadier General Bryan Roberts, Major General Ralph Baker, Rear Admiral Charles Gaouette, Lieutenant General David Holmes Huntoon, and General Carter F. Ham — all resigned or were dismissed around the same time, during the government shutdown of 2013. Coup or counter-coup, or just spring cleaning, the media did not report, nor speculate.

One wonders how secure the G20 leaders felt, when they learned they were being bugged. "Oh, so *now* you want our support on Syria? Really? Didn't you hear it last week when I told my cabinet we'd rather be buggered by rabid wolves than cooperate with you?"

We say "security" to mean the protection of our secrets, as they fly across the Internet, as well as the warm fuzzy feeling that gives us. The Spider has worked hard to strip away that protection. I'll explain something of that protection and how it broke. We'll look at three kinds of security, and I am going to use some dirty language, so if you don't like that kind of thing, please skip a few pages:

- One person, keeping secrets for themselves (private files). This means *encrypting* the data with a *symmetric key*, which is a key that both locks and unlocks the secrets.
- Two people, talking to each other (phone, email, chat). This means *authenticating* both parties, to be sure who is speaking, and using *asymmetric keys* to encrypt and decrypt the data. That is, one key locks, and another key unlocks.
- One person, talking anonymously to a crowd (whistle blowers, bloggers), or accessing a website anonymously. This means *anonymizing* the origin of data sent to the Internet, i.e. removing all details about the IP address used on the original sender computer,

180 http://www.reuters.com/article/2013/10/16/us-usa-nsa-transition-idUSBRE99F12W20131016

while still making it possible for replies to go back to that original computer.

A symmetric key is usually a string of words ("The R4in F4lls M4inly In Sp4in") that is hashed into a long number, used as the key. It is easy to crack any symmetric key. You just take a person who knows it, and threaten them, or beat them. This is called the "rubber hosepipe attack." When you carry encrypted data into the US, for instance, you pass a no-man's land where agents of the Customs and Border Protection (CBP) can stop you, seize your equipment, and ask you nicely for the keys. If you don't cooperate, you will be charged as a criminal. The UK has the same system.

Asymmetric keys are more fun. These make use of weird maths where two very long numbers work together; one to turn data into gibberish, and one to turn that gibberish back into data. It's like turning cement powder into concrete by adding water, and then turning concrete back into cement powder by applying heat. So I can tell people, "use heat" and give them cement blocks. I keep "water" secret. When I get two magic numbers that work together, A and B, and tell people about B, then I can encrypt my data with A and share it. Anyone who has B can decrypt it, and they know it came from me.

This gives us secrecy, thanks to the encryption, and also "authentication," which is the knowledge that the data really came from me, and not an impostor. There is little point in encryption if we can't be sure of the sender. There's a small catch: you also need to be sure that B is really my key, and was not switched by some "man in the middle," or MIM.

For asymmetric keys to work at all well, those encryption keys must be exchanged securely, which creates an interesting Catch-22 that attackers exploit. The keys must also, and this is very important, be really random and unguessable. If you can guess the keys, the whole encryption exercise is for naught. Even if your guesses are very vague, it can make the difference between trying different keys for an hour, or for 50 years. When we use random number generators that have

some predictability, we're vulnerable to anyone who knows those weaknesses. When done on purpose, this creates a "backdoor" into an otherwise secure system.

So random number generators are more than a mathematical curiosity. They can make the difference between secrecy and exposure, and in extreme cases, life and death. A high-profile argument in 2011 over an Intel-provided patch to the Linux random number generator led to maintainers quitting the project[181] and accusations of backdoors, and some concern when the NSA's backdoor strategy became public in 2013. Linux at least benefits from open discussion and massive visibility. If someone tries to sneak in a backdoor, it cannot survive long.

This isn't the case with closed, commercial products, where backdoors can survive for many years. One of the world leaders in asymmetric security products is EMC Corporation, which owns RSA Security[182]. It makes SecurID tokens, which are widely used to protect access to corporate networks, and a commercial library, BSAFE, widely used in products.

Since at least 2006, these products used a random number generator called Dual_EC. This algorithm was chosen by the National Institute for Standards and Technology (NIST), despite its being extremely slow. Some cryptographers suggested at the time that it had weaknesses — in other words, you could predict the keys it would generate. Nonetheless, NIST standardized it, and that standard went through the International Standards Organization (ISO) in Geneva, becoming a government-approved standard worldwide. EMC shipped its products and these went into widespread business and official use.

181 http://thread.gmane.org/gmane.linux.kernel/1173350/focus=1173517

182 http://en.wikipedia.org/wiki/RSA_Security

Then in September 2013, the New York Times wrote[183] that, "an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA." Not only had the NIST accepted the NSA's recommendations of a weak, slow algorithm. They had effectively given the NSA sole authorship of the standard.

Given that most cryptographers — by nature, a skeptical lot — stayed away from Dual_EC, it is significant that the NIST (supposedly the experts in this field) didn't speak up. Much the same observation goes for RSA Security, who are most *definitely* the presumed experts in this field. They patented asymmetric cryptography, after all.

Today, NIST is largely discredited as a trustworthy authority on security. The most careful people also stay away from any security technologies that are not independently designed, and fully verifiable. Hence the emotional discussions on the Linux lists about that random number generator patch. In 2013, any security product that isn't open source isn't credible.

We're still not secure, however. Let's say we can generate *really strong* keys that no-one could ever guess, immune from rubber-hose attacks, and hard enough to crack that it would take a zillion years to try all combinations. It's still trivial to break such security, if I can do a man in the middle attack.

A MIM attack takes advantage of the fact that even if we can create secure keys, we need some way to exchange them. It's like me sending the key to my house in the mail to a person coming to stay. An attacker can open the mail, take out my key, substitute his, with a letter containing an impostor address. The poor visitor will come to the wrong house, enter, and know nothing. Meanwhile the attacker can enter my house, pretending to be the visitor.

---

183 http://arstechnica.com/security/2013/09/new-york-times-provides-new-details-about-nsa-backdoor-in-crypto-spec

The industry's answer to MIM attacks is something called "public key infrastructure" or PKI, which means we give our keys to someone we can trust to hold them. There are about 50 such trusted "certificate authorities," or CAs, and their public keys are embedded in our web browsers.

When the browser trusts a certificate authority's key, it can trust the key of a server that was "signed" by the CA. The whole thing works, more or less, yet has two big problems. One, it's expensive, since CAs have a soft cartel which they can exploit by charging hundreds of dollars for a few seconds of CPU time. Two, it's not really secure after all. Eggs in baskets attract foxes, and CAs are a juicy target for the Spider.

In 2011, the Dutch CA DigiNotar[184] was found to be issuing fraudulent certificates following a hack. Two years later we discovered that hack was, probably, the work of the NSA. Who would have guessed it. If you can take over a CA, or start your own CA, you can run MIM attacks on anyone who buys certificates from you. And a little later, security researcher Bruce Schneier reported that[185] the NSA "covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format."

PKI, like any centralized infrastructure, is vulnerable to intrusions, and simple brute force. While it may be hard to convince a Dutch CA to cooperate with US military intelligence, it's doubtful that US certificate authorities have the same freedom to say "no." We've seen what happens to firms that try to fight the Spider[186].

There are in fact ways to make that secure phone call. For example I spent much of 2013 building such security into ZeroMQ, so that it became much easier to build highly secure communications systems. However, as long as we connect over our domestic or office Internet

184 http://en.wikipedia.org/wiki/DigiNotar

185 https://www.schneier.com/cgi-bin/mt/mt-search.cgi?tag=man-in-the-middle%20attacks

186 http://lavabit.com/

connections, we're vulnerable to "metadata capture." Perhaps the Spider can't read what I'm typing, yet it sees who I'm sending it to, and it sees when that person replies. And the Spider of course collects metadata without even apologizing. As the NSA explains to an indifferent Congress and a lazy media, that is not even real data, and does not count as surveillance.

The metadata on who we talk to, and when, and for how long, is of course enough to create a rich file. In the story of the Spider using its surveillance to blackmail politicians and competitors, metadata is more than powerful enough. General David Petraeus[187] was a 4-star general with 37 years of experience, in charge of coalition forces in Iraq. In June 2011 he took over as director of the CIA, in a 94-to-0 unanimous vote. And a year and a half later, he quit, in a sex scandal uncovered by the FBI through an email trail.

I'd say the FBI was just doing their job, except that investigations against powerful people for serious crimes seem never to happen. Infidelity... well, if that was reason for politicians to step down, there would be few leaders left. Whether Petraeus was pushed, jumped, or was just honestly embarrassed, the contents of those emails didn't matter as much as their very existence.

Peeling the Onions

The more paranoid and devious citizens of the digital world know, of course, that metadata is precious, and have worked for years to build anonymity networks, above all one called Tor[188]. Tor was originally a US Navy and DARPA project. The funding for the Tor Project still comes in large part from the US State Department, which sees it as a vital tool for foreign policy.

Tor uses layers of encryption to hide the origin of packets sent to the Internet. It gives journalists, activists, and whistle blowers a way to publish without being tracked and punished. Privacy isn't a luxury

187 http://en.wikipedia.org/wiki/David_Petraeus

188 https://en.wikipedia.org/wiki/Tor_(anonymity_network)

when simply writing about a sensitive topic like religion can result in corporal punishment and imprisonment[189].

Tor creates a network of "onion sites," also called the "Deep Web," accessible only via a Tor browser. The name "onion comes from the way the security works, layer by layer. The Deep websites are invisible to normal Web users, you cannot open them in a browser. The most famous such site was the Silk Road[190] marketplace, mainly used for selling drugs by some accounts, guns and worse by other accounts.

The Tor network also lets its users connect onwards to real websites, through so-called "exit nodes." An exit node acts as a bridge between the Tor network on one side, and the open Internet on the other side. These exit nodes range from small hobbyist servers handling a handful of connections at once, to massive servers handling thousands.

Tor has a number of weaknesses. Technically, it can be secure, if you are an expert user, and you stick to Deep websites. You must run Tor from a separate virtual machine, and wipe that after each use. For instance, having a Silk Road alias on your computer would be incriminating evidence. Most users will however simply run it from their normal machine, and will access normal websites. This makes it possible to track them.

The second technical weakness is the reliance on exit nodes for outgoing access. There are perhaps 1,000 exit nodes worldwide, a quite small number. Controlling a fraction of these would let the Spider get the real Internet addresses of tens of thousands of Tor users. The NSA can either hack into a Tor exit node and take it over, or they can (and one assumes, do) set-up their own Tor exit nodes. It costs relatively little. The bigger the budget, the more traffic one can tap.

As Dan Egerstad, a Swedish security consultant, notes, "If you actually look in to where these Tor nodes are hosted and how big they are, some of these nodes cost thousands of dollars each month just to

189 http://www.hrw.org/news/2013/07/30/saudi-arabia-600-lashes-7-years-activist

190 https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

host because they're using lots of bandwidth, they're heavy-duty servers and so on. Who would pay for this and be anonymous?"

The other half of taking control of the exit node network is to deter honest operators. It's a fairly simple exercise. If a Tor user distributes child porn via an exit node, the exit node operator can be held responsible[191]. Tor is practically designed to plant evidence on exit nodes.

The third weakness with Tor is that it attracts criminals, which makes any Tor infrastructure a standing target for the authorities. As Wikipedia notes: "Tor can also be used for anonymous defamation, unauthorized leaks of sensitive information, and copyright infringement, the distribution of illegal sexual content, the selling of controlled substances, money laundering, credit card fraud and identity theft."

And so the Deep Web is under attack from the security services. In August 2013, the FBI took over[192] the largest Tor hosting site, called Freedom Hosting. This company hosted half the onion sites in the Deep Web, licit and illicit alike. By placing malicious Javascript code on these onion sites, the attackers were able to capture their users' Internet addresses. A day later, the whole infrastructure went down. At the same time, its founder was arrested on child pornography charges. A little later, security researchers found that[193] the Javascript code sent the captured information to an NSA machine.

From pedophiles to anyone using anonymous networks, the net only gets larger, never smaller. The leaking of an NSA address in such a carefully-orchestrated exercise does not seem accidental. It would be so trivial to hide. More likely, it's meant to send the message, "We are watching."

---

191 http://www.techdirt.com/articles/20121130/07495221185/tor-exit-node-operator-charged-with-distributing-child-porn.shtml

192 http://www.twitlonger.com/show/n_1rloouu

193 http://arstechnica.com/tech-policy/2013/08/researchers-say-tor-targeted-malware-phoned-home-to-nsa/

People speculated at the time that this attack on Freedom Hosting was the prelude to an attack on Silk Road. It made sense, since Silk Road was a major attraction for newcomers to Tor. As long as it existed, people would trust and invest in Tor, and work around any tactics the authorities invent. Taking down Silk Road would hurt Tor's growth and future badly. In theory, a Deep website like Silk Road cannot be found and shut down by the authorities. However in October 2013, the FBI arrested its operator, Ross Ulbricht, aka "Dread Pirate Roberts",[194] and seized the Silk Road servers.

The first death of Silk Road — for I'm sure it will be resurrected — and subsequent worldwide prosecution of dealers who used it puts a large question mark over Tor. The FBI's explanations of how they tracked Ulbricht through his clumsy on-line activity smells of "parallel construction"[195], aka "intelligence laundering," and the NSA's handy set of Internet spy tools.

More encryption is not the answer, though. It just makes things harder for ordinary users. In the end, any community that depends on centralized infrastructure, no matter how encrypted, is vulnerable. The problem is that those centralized servers are a single point of failure. Arrest one man, and you take down half the Deep Web. And, that we still have to connect to the Internet somehow. That means our IP addresses can be tracked, and our activity logged, by our broadband provider.

The Dangerous Young Men

Realistically, things will have to get rather worse before the mass market and business will invest seriously in a safer alternative to today's Web. Until then, it will be the idealists, privacy freaks, cryptographers, political performance artists and busybodies like myself who

194 http://rt.com/usa/silk-road-bitcoin-shut-650/

195 http://www.forbes.com/sites/kashmirhill/2013/10/08/did-the-nsa-help-with-the-silk-road-investigation

build such things. I've spent the last years investing in ZeroMQ, a core technology for secure decentralized communications.

It will take a lot of work to rebuild the web, no matter what technology we use. One thing the Internet has in large numbers, however, is capable young men with a rebellious streak. The chemistry of change just requires that these Dangerous Young Men focus their attention on the challenge of the decentralized Internet. Once it's seen as a plausible direction, there is no stopping the reaction.

Indeed, when the Greedy Old Men try flatly to stop the reaction of change, it just makes it run faster. It's a recurring pattern of conflict between the old men and the young ones. Indeed, an ancient one that is universal in myth and history, and embedded in the fiber of our species. There are not many old revolutionaries, nor young reactionaries. Nor is this a women's game until it hits wider society. There is something disposable about the young human male which makes it profitable for him to take greater risks.

The story starts with a couple of young upstarts who hack together something that challenges the old order. In history it was perhaps a political party, a forum, or a business. These days it's more likely to be a website or a piece of software. For a while nothing happens, and that's mostly how it stays. Yet just now and then, that little seed of a challenge takes root, and grows. It brings in more young men, and suddenly people are talking about it, and the old men — not good listeners at the best of times — get to their feet and start to ask questions.

Hogwash, say the old men, as they listen. That'll never fly. And then it does. As Nicholas Klein said[196] in an address to Amalgamated Clothing Workers of America[197], in May 1918, "First they ignore you. Then they ridicule you. And then they attack you and want to burn you." So the old men move to attack the upstarts, calling in favors, so

196 http://www.barrypopik.com/index.php/new_york_city/entry/first_they_ignore_you_then_they_laugh_at_you_then_they_fight_you_then_you_w/

197 http://en.wikipedia.org/wiki/Amalgamated_Clothing_Workers_of_America

security comes to beat up and arrest the ringleaders, and the press paints them as degenerates. Klein added, "And then they build monuments to you," though that was arguably just to warm up the crowd.

You'd think that would be the end of it, yet rather than quash the dissent, this police action has a perverse effect. Suddenly there are martyrs, and a tenfold increase in dangerous young men looking for action. What was a sideshow becomes the main attraction and before they know what hit them, the old men are running for their lives, their villas burnt, their families scattered. Conflict can attract, rather than repel.

A classic example of such a conflict on the Internet was the music and movie's long fight to stop sharing of their commercial products on the Internet. This so-called "War on Piracy" was perhaps the first real battle between old industrial businesses, and the new digital world. Incidentally, "piracy" is an old insult against copyright and patent violators, dating back to at least 1850. In those days, lobbyists used it to describe Dutch and Swiss firms who copied industrial processes from the Americans and French.

In "Wealth of Nations", I explained how all property is based on some level of coercion. We tolerate the State because it's the only plausible way to get balanced, symmetric coercion. The music industry has turned asymmetric coercion into a core business strategy. It pushes young artists into signing deals, and uses "collecting societies" to suppress an independent music industry. These collecting societies take fees from radio stations, clubs and cafés, concert promoters, and so on, and pass these onto their members, who are the established music businesses.

You are either in the system, and you play by the rules, or you are outside, in the cold. Some musician friends, invariably poor like every musician I ever met, explained that they had to pay collection society fees when they played a concert *of their own original music*. They could otherwise have stayed off the radar, signed no contracts, sold no CDs in the high street shops, played no concerts in the big venues.

The music industry made, and still largely makes, its profits by controlling the whole business process from raw artist to final user experience, allowing no real competition at any point along this chain. They gouge the artists so badly you would think by now no artist would even talk to them. Yet, there are always more young eager faces waiting in line. Artists seem to scramble over each other to be exploited. Just as the diamond industry keeps its prices high by stockpiling rough stones that it never sells, the music industry signs artists simply so they cannot play on the free market.

When digital society realized they could bypass the music industry's antiquated and painful distribution process, there was a kind of ecstatic explosion of joy. I remember looking at my CD collection in 1995, wondering why I could not store and play all that digital music on my computer. Apart, that was, from the small detail that one hard drive could hold about two-and-a-half CDs.

The old men of the music industry confronted the upstarts somewhat like the Titanic confronting the iceberg. You can see the innocent arrogance of power hitting the raw uncaring brutality of nature, and sinking, slowly yet surely, into the icy water. Unlike the Titanic, though, the sinking of the music industry is still ongoing after two decades.

Here are the headlines of the sinking. It all starts when Sony and Phillips release the audio CD format, which is a digital audio disc, and a little later, CD-ROM, which is a format for data. An enterprising Taiwanese CR-ROM maker, whose name I forget, realizes they can make the audio data available to applications with a trivial pin-out. Connect a little cable to your sound card, and suddenly you can read the CD data on your computer! 650 megabytes of raw audio data, larger than most hard drives at the time.

Then all hell breaks loose, in a slow, shambolic kind of way. We saw the Fraunhofer Society's release of MP3 encoders in July 1994. We saw the rapid birth and death of Napster (June 1999-July 2001), MP3.com (July 1999-May 2001), Gnutella, FastTrack, WinMX, AudioGalaxy,

and AllofMP3, to name a few, finally landing us with BitTorrent as the uncaring iceberg.

Over a decade, copyright law shifts gradually, country by country, from a civil offense, to a criminal one. The powers of the State gradually come into play. The police seize servers, arrest operators, bring down websites. While the State seems to enjoy its role as cartel enforcer, the criminalization of file sharing does nothing to stop the sinking of the music industry. The arrests and court cases continue, yet for every torrent site taken down, ten more spring up.

Slowly, the industry accepts an "all you can eat" model and by 2008, Spotify starts a legal commercial streaming service. As always, it is the studios who get the profits, not the artists. In 2012, after a long battle, a Minnesota woman agrees to pay the RIAA $220,000[198] for downloading 24 songs. The recording industry vaguely realizes the insanity of its lawsuits, yet cannot resist one last dawn raid, sending a Finnish police squad[199] to seize the laptop of a 9-year old girl. Her father had refused to pay a EUR 600 fine, and sign a non-disclosure agreement for downloading one song from the Pirate Bay.

Has the music industry survived? That is debatable. Downloading music is easier than ever, and by extorting punitive damages against women and children, the music industry has shot itself in both feet, reloaded and shot again. It will never recover public trust and support. YouTube has given up policing music, and indeed, has replaced MTV (remember that?) as the place for music videos. The RIAA has switched from suing its users to mass takedown notices against firms like Google, also a failing strategy[200].

It was never about stealing, it was about convenience and fairness. Digital content should be easy, and it should be plentiful, and it

198 http://www.theguardian.com/technology/2012/sep/11/minnesota-woman-songs-illegally-downloaded

199 http://torrentfreak.com/police-raid-9-year-old-pirate-bay-girl-confiscate-winnie-the-pooh-laptop-121122/

200 http://www.outsidethebeltway.com/riaa-takedown-strategy-backfires/

should be priced for mass consumption. People happily pay Spotify for unlimited streaming on all our devices, which is anyone ever wanted in the first place. My Spotify account costs me less than 1% of my old CD collection, per year.

After spending 15 years lobbying at the highest levels to have a majority of Internet users criminalized, the music, movie, and TV industry is starting to realize that the so-called pirates are really not the problem. The real problem is that in a world filled with free and interesting material, their commercial content, like newspapers, is becoming old-fashioned, and irrelevant.

The realization is strongest in the television industry, particularly businesses like HBO, that sell highly-addictive series to subscribers. HBO's most popular show as I write this is Game of Thrones, a cracking swords-and-dragons political epic. It is also the most pirated TV show ever.

Speaking of this[201], the CEO of Time Warner (owner of HBO), said, "Our experience is, it all leads to more penetration, more paying subs, more health for HBO, less reliance on having to do paid advertising — we don't do a whole lot of paid advertising on HBO, we let the programming and the views talk for us — it seems to be working." So piracy is not hurting sales of TV shows, and instead emerges as the cheapest and most effective way to increase them. Of course we always knew this. However, it's nicer when the CEO of a TV company says it out loud.

For the music industry, the same logic is starting to apply. I explained in "Wealth of Nations" how the smart record labels are using YouTube to promote their hits by encouraging remixes. Perhaps the music industry will design addictive music products as the TV industry is doing, and sell these to subscribers.

For the movie industry, it seems clear that without the Internet to promote their new movies, YouTube for the trailers and reviews, and

201 http://www.businessinsider.com/time-warner-ceo-people-pirating-game-of-thrones-is-better-than-an-emmy-for-hbo-2013-8

IMDB for the discussions, theaters would be getting empty. And without Pirate Bay to keep old movies available, the movie industry would slowly fade from our minds.

However the realization that the upstarts and their aggressive deconstruction of the past are essential for the future takes a long time to percolate through the stone minds of the old men. Indeed, the time scales suggest that the old men never learn, they are instead slowly replaced by younger men who "get it" and find ways to turn the "dangerous" platforms and technologies into profitable and acceptable businesses.

The pattern of hostility between dangerous young men and old reactionaries has played out over and over. My apologies to my female readers. This caricature of revolution (technological or other) as a mainly male game is what we see. There are many women, dangerous or not, in technology, however it seems to be mostly the men who stick their heads up, and get them chopped off.

The crushing of the Silk Road is following the classic plot line. As it did with in the Napster case, smashing a popular underground platform is unleashing a many-headed monster. Brute force isn't a deterrent to the dangerous young men, it is an irresistible challenge. A harsh response from the authorities is a badge of success. And indeed a few weeks after the FBI took down the original Silk Road, its users prepared to launch a new set of platforms[202].

One commentator, who worked for a short-lived Silk Road competitor called Atlantis, wrote[203], "What's striking to me as an outside observer is there seems to be no shortage of well educated American males in their late 20's (Manning/Snowden and now Ulbricht) willing to sacrifice bright futures and their own personal liberty to highlight the draconian laws and downright totalitarianism being inflicted

202 http://techcrunch.com/2013/10/04/deep-web-users-are-ready-to-launch-silk-road-2-0/

203 http://atlantisblog.org/silk-road-subdued-but-this-ex-blackmarket-employee-believes-they-only-released-a-monster/

by their government on the populous." And then, more dramatically, "I believe I am now witnessing a full revolution in progress and I for one will be sticking around to document it."

The Fires of Change

Sometimes the reaction of change burns hot, engulfs broader society, and presents a hotter challenge to the authority of the State. When this happens, the State can react murderously. 45 years ago the Mexican government, faced with ongoing protests in the Tlatelolco area of the capital, shot large numbers of students, organizers, and bystanders[204] in one night, killing several hundreds, and arresting over a thousand, many of who still languish, a lifetime later, in the Mexican gulag system. According to unofficial reports, the firestorm was set off by government snipers shooting at nervous soldiers, who responded by firing at protesters and bystanders.

States do this kind of thing when they don't see a way to keep a lid on dissent. One would hope that it happens less and less over time, yet we're seeing a broad and deep militarization of civilian law enforcement in the US. That is either a vast boondoggle for the defense industry, addicted to selling weaponry on a planet that has less and less need of it, or something rather more sinister.

I rather like the boondoggle theory because it fits with the usual habits of men, to steer every exercise towards private profit. It's much more plausible to assume that cities are buying loads of expensive rifles, ammunition, and armored vehicles because someone is getting a 10% or 15% kickback, than because there are evil lizard overlords plotting our ruin.

Having said that, it is reckless not to plan at least for the worst, even if we hope for and assume the best. It is the same reason we must build surveillance-proof networks. I don't expect a car crash every time I leave the driveway. Still, I lock my seatbelt every time I close the car door. Prudence is cheap. Kinetic energy dispersing in organic tis-

204 http://en.wikipedia.org/wiki/Tlatelolco_massacre

sue is costly. So even if we don't really believe that story of the Para-state and its Spider, let's just imagine that out there, somewhere, an old man reads "a full revolution in progress," and reaches for his sidearm.

When faced with a revolution, you don't go out and shoot or arrest peasants. Peasants are the stumbling dead of the apocalypse. They look strange, and smell, and possibly drop bits of rotting flesh as they pass. However, they're basically harmless so long as you don't let them touch you, or overwhelm you with sheer numbers. What you have to watch our for are the infected crazies[205], who "furiously and relentlessly pursue non-infected persons demonstrating notable speed and agility combined with complete disregard for self preservation." And while the world is filled with people infected with crazy ideas like Freedom, the worst of all are the spoiled, over-educated, reckless youngsters we call "students."

It's literally step #1 of "How to Control Your Revolting Population in Five Easy Steps," the popular teach-yourself manual for aspiring dictators. You locate the students, you provoke them into action with a few arrests, shootings, and bans, and you then bring in the army to shoot them en-masse and bury, sorry, *arrest* the survivors. It works every time, partly because fast-moving metal projectiles always beat flesh, and partly because the mass of people fundamentally don't like students and can ignore a lot of violence against them. Students are loud, they smoke pot, they have long hair, they don't work (Horror shock probe!), and unforgivably, they have more sex than normal people do.

While universities are often the scene of protests, the out-and-out shooting of protesting students is thankfully rare. Googling, I found Tlatelolco, Kent State, Thammasat, Tiananmen Square, Nasarawa, Abeokuta. Not a very long list for decades of student discontent. However I recall vividly, a short time before the Rwandan genocide of 1994, watching a TV report of arrests made in Kigali of Tutsi "sym-

205 http://zombie.wikia.com/wiki/Types_of_Zombies

pathizers." As the camera panned across the jail floor, I saw a close friend sitting there, recognizable despite his shaved head. A musician, he'd lived with us in Antwerp just a few months earlier, returning to Rwanda to help his family there. We never saw him again. His crime: to be an intellectual, a voice, a focus of dissent.

Most repression is invisible unless you are close by. Despite the caricatured apathy towards students that I drew, it is the educated 20-somethings that are the brains of any revolution, and the main targets of selection repression. The Para-state is expert at luring them out and crushing them in elegant mazes of confusion. The Para-state may be incompetent when it comes to science, maths, ecology, or even basic humanity. However, one thing that they are truly experts at is holding onto power.

The Egyptian revolution of 2011 was a classic example. We saw non-violent protests by the middle class, during the Arab Spring, turning into a soft revolution against a corrupt leadership. We saw these protests, the first wave, encouraged by the West and tolerated by the military. We saw the dictator Mubarak deposed and placed into house arrest. Then there were elections that, tragically, transfered power to the extremist Muslim Brotherhood.

The MB used their new power to tear up the constitution and enact intolerable laws. What a catastrophe! The army, with regret, stepped in. The extremists fought back. We saw violence, deaths, arrests. We got bored. Yet still, we applauded as the MB was dismantled in a river of blood. No-one wants Islamic extremists in power! Fifty dead in a day. A hundred. Who kept count? The only good terrorist is a dead one anyhow. Few of us however, in the chaos and the confusion, saw what happened to the leadership of the first wave. They just disappeared.

There was no real revolution in Egypt, no real change of State. What we saw were, I believe, useful idiots and egomaniacs being given rope, and then hung by it. And, more usefully, the real targets — the young leaders of the first wave — being disposed of while no-one was

watching. I assume the MB was encouraged by agents provocateurs and slush funds, that the elections were rigged, and that the real goal was always the continuity of the dictatorship, and the real targets were those dangerous 20-somethings.

There is, in late 2013, at least the visible start of a move against the dangerous young men of the Internet. How deep and wide that move is, we don't know. I believe the Spider moves slowly yet very deliberately. Small moves in a new direction presage large events. One of those directions is the creation of an Internet with two sets of laws, one for the rich and one for everyone else.

The Protected Computer

Over Thanksgiving weekend in 2011, the Senate passed the National Defense Authorization Act[206] (NDAA). Senator Lindsey Graham, one of the bill's sponsors, said about it on the Senate floor, "the statement of authority to detain, does apply to American citizens and it designates the world as the battlefield, including the homeland."

As Amber Lyon reports[207], "The NDAA gives the federal government the power to behave like dictators and arrest any American citizen, or anyone for that matter, without warrant and indefinitely detain them in offshore prisons without charge and keep them there until "the end of hostilities."" Award winning investigative correspondent Amber Lyon infamously revealed how CNN took money to decide what stories to report[208].

She continues about the NDAA, how Barack Obama "lied to the public and said he would veto the NDAA's indefinite detention clauses. Instead, he surreptitiously signed the NDAA into law on Dec. 31, 2011 while most Americans were distracted celebrating New

206 http://www.aclu.org/blog/national-security/senators-demand-military-lock-american-citizens-battlefield-they-define-being

207 http://amberlyonlive.com/2012/12/09/why-i-say-fuck-the-ndaa/

208 http://www.theguardian.com/world/2012/sep/04/cnn-international-documentary-bahrain-arab-spring-repression

Years Eve." The NDAA was clearly a discrete declaration of war... and aimed at who exactly?

Let's go back to one of the first attempts by lawmakers to control the new digital world. The 1986 Computer Fraud and Abuse Act (CFAA, 18 USC § 1030[209]), makes it a federal crime to use a computer "without authorization or exceeding authorized access," and then steal or modify information. This sounds fair enough. The law looks reasonable, and reads like an honest, if somewhat outdated, attempt to stop people doing Bad Things on other peoples' computers.

However, like all laws, the game is in the spirit, not the words. Who defines what "authorized access" is? Who defines the value of information? There is a lot of focus on "protected computers"[210], a term the law defines thus:

> *2) the term "protected computer" means a computer — (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;*

It is an extremely broad claim of authority: touch any network switch, router, WiFi access point, server, or cloud service *anywhere in the world* in a way that affects any US business, especially the financial sector, or the US government, and we will treat you as a criminal.

Further, it is the actual use of the computer that is the crime. Let me explain that. What you actually *do* on the computer may also be a

209 http://www.law.cornell.edu/uscode/text/18/1030

210 http://en.wikipedia.org/wiki/Protected_computer

crime, or may not. That's beside the point. Only in 2013, more than 25 years after the law was passed, was section (a)(1) used for the first time, in the prosecution of Chelsea née Bradley Manning[211].

It is a bad sign when prosecutors start pulling on unused old laws to chase down new threats. To start with, it shows the old law was wrongly designed. The perceived threat in 1986 was teenagers hacking into defense systems and starting a nuclear war. Clearly in a quarter century, that never happened, outside of the movie theater. Do lawmakers believe that Hollywood makes documentaries? And then, it's bad because prosecutors start to push at the limits of language and meaning to get the convictions they want. It is a classic lawyer's game: you define a term, and then I will make it mean precisely the opposite, with the fewest court cases possible. It is bad science to gather data to support a hypothesis, and it is bad justice to twist a law to support a prosecution.

In April 2013, Cory Doctorow wrote[212], of the US Department of Justice (DoJ)'s persecution of the young activist Aaron Swartz, the archetype of a Dangerous Young Man:

> *When my friend Aaron Swartz committed suicide in January, he'd been the subject of a DoJ press-release stating that the Federal prosecutors who had indicted him were planning on imprisoning him for 25 years for violating the terms of service of a site that hosted academic journals. Aaron had downloaded millions of articles from that website, but that wasn't the problem.*
>
> *He was licensed to read all the articles they hosted. The problem was, the way he downloaded the articles violated the terms and conditions of the service. And bizarrely — even though the website didn't want to press the matter — the DoJ decided*

211 http://www.eff.org/deeplinks/2013/07/bradley-manning-was-punished-more-merely-because-his-leaks-involved-computer

212 http://boingboing.net/2013/04/08/today-we-save-the-internet-a.html

that this was an imprisonable felony, under the Computer Fraud and Abuse Act, which makes it a crime to "exceed your authorization" on any on-line service.

The CFAA would make a young girl a criminal, if she was in the US, for lying about her age on her Facebook profile, and thus receiving information she is not entitled to. Children are an unlikely targets of prosecution though, I hope. The real focus of the CFAA are the "nihilists, anarchists, activists, Lulzsec, Anonymous, twenty-somethings who haven't talked to the opposite sex in five or six years," using the words of Michael Hayden, former director of the NSA and the CIA. Hayden ran the NSA when it switched from foreign military intelligence to domestic spying. Hayden is, dare I say it, a Spider man.

Ironically, for a long time, the NSA was seen as one of the best places to work, if you were a smart technology-oriented nerd with particular talents. For years, the agency cultivated its image as the quiet force for good, the honest policemen of the Internet. It proposed "stronger" (hah!) security standards and pushed them through US and international standards organizations. Young men like Aaron Swartz were the best possible talent the agency could ask for, to keep the Internet safe for Honest Citizens.

Glyn Moody writes[213], "as the NSA is now finding out, those same hackers are increasingly angry with the legal assault on both them and their basic freedoms."

In his "nihilists and anarchists" speech[214], Hayden made it clear that he considered the "twenty-somethings" to be the next terrorists:

Mr Snowden has created quite a stir among those folks who are very committed to global transparency and the global web,

213 http://www.techdirt.com/articles/20130805/02354124062/us-government-war-hackers-backfires-now-hackers-wont-work-us-government.shtml

214 http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden

kind of ungoverned and free. I'm just trying to illustrate that you've got a group of people out there who make demands, whose demands may not be satisfiable, may not be rational, may not be the kinds of things that government can accommodate. They may want to come after the US government, but frankly, you know, the dot-mil stuff is about the hardest target in the United States. So if they can't create great harm to [military websites], who are they going after? Who for them are the World Trade Centers? The World Trade Centers, as they were for al-Qaida.

In December 2010, PayPal, Visa, and Mastercard (among other firms) froze WikiLeaks' account, cutting off donations to that site. In retaliation, Anonymous organized "Operation Payback," a "distributed denial of service" attack on those firms' web servers. Thousands of people around the world ran scripts on their PCs that sent request after request to PayPal's servers, overloading them, until no-one could use them. Under the CFAA, this gave the FBI a mandate to arrest them and prosecute them, which started about three years later, in October 2013.

Operation Payback was very significant. It was ostensibly a non-violent protest against the banks and payments processors who had tried to strangle WikiLeaks. However, what it really signified was the escalation of the war between the Spider and Para-state, and the digital revolution.

Anonymous, worthy of a book in themselves, had sharpened its teeth on Scientology, no easy target. In 2008 there were maybe half a million Scientologists in the world (claims varied from 100,000 to an unlikely 20 million). Then in February, over 9,000 protestors came out onto the streets and confronted this organization. By 2013, the largest pro-Scientology events — such as in Clearwater, FL in November 2013 — had no more than 2,000 or 3,000 people.

And this demolition of Scientology, one of the most powerful and feared cults, cost nothing, no private investigators, no weapons, no vi-

olence, and indeed very little confrontation. Without implicit popular support, Scientology discoved that all their money was worth nothing.

So Anonymous — an idea, not an organization — now attacked the financial system, and by implication, the US Government. The arrest of young male protesters — including a 16-year old Dutch boy — and indictment for high crimes against the State is a classic old men versus dangerous young men story line.

We've seen that Bank of America conspired with private companies to, in their own words, "Commit cyber attacks against the infrastructure" of wikileaks.org. This, we see, is perfectly acceptable. However, to conduct the equivalent of a non-violent street protest against PayPal's Internet headquarters is a federal crime leading to arrest and prosecution. There is not even the pretense of impartiality.

Knowing in 2010 that the Spider was watching every click, those young men would have been rather more careful. Since it took over two years to pounce, we can assume there are more international "cyberterrorism" warrants in the pipeline. The result will be like pouring water on an kitchen grease fire. The coming arrests — like that of Jeremy Hammond, taunted and guided by FBI assets into the hack on HBGary Federal — will create martyrs and inflame the dangerous young men who think of themselves as Anonymous.

The Golden Rule

The criminalization of on-line activists may seem new. However, the principle of "you are either our friend, or our enemy" is an old staple of every conflict, as any child of divorce knows. The one area where the Spider sees a particularly sharp difference between its friends and its enemies is the financial industry. Before 2008 we perhaps didn't see how profoundly the Para-state depended on its banking sector, how far it would go to protect the banks from their own greed, and from the laws of the land[215].

215 http://www.bloomberg.com/news/2013-07-02/hsbc-judge-approves-1-9b-drug-

He who controls the gold makes the rules, and anyone who wonders what might happen to new virtual currencies like BitCoin would be wise to read history. The independent banking sector, cash economy, and virtual currencies are not friends to the Spider, thus are its enemies. If this was not clear before September 11th, it certainly became clear after that. However, we'll start our money story a few years before 9/11, in the last years of the twentieth century, as governments of the West started to crack down on cash transactions and banking secrecy.

It used to be that you could walk into almost any bank in Europe a check, or cash, and open an account under an assumed name, without ID. "Can I open an account?" "Yes, certainly. Do you have identification?" "No, though I do have this check." "That'll do nicely, sir."

This was a cross-border specialty. For decades, Germans seeking to avoid the high taxes of their country could hop over the border to Austria, open an anonymous numbered account, and put undeclared cash income there. High taxes and old laws left Europe littered with convenient little tax havens: Andorra, Monaco, Luxembourg, Jersey, Malta, Liechtenstein. Even Belgium welcomed tax refugees from the Netherlands, as did Germany from Austria, and Switzerland from anywhere in the world and especially from corrupt foreign dictatorships.

Anti-money laundering (AML) regulations ended such liberties. Ostensibly, the purpose was to catch drug traffickers, by requiring identification for any transaction, and justification for any transfer over $10,000. The real goals were more likely to break the cash economy, stop tax evasion, and allow authorities to correlate banking information across Europe. The real payoff for the banks was increased cash flow.

Arguably though, a single currency and the single European market makes money laundering easier, not harder. Drug money of course

---

money-laundering-accord.html

didn't stop flowing in the 1990's, and it doesn't take a genius to see how to get around the AML controls.

Say a street dealer sell drugs — sugar-coated croissants, perhaps — in Paris for EUR 1 million in undeclared cash. He drives with this dirty cash in a bag to Vienna, then hops across the border to Bratislava, the capital of Slovakia, famous for its investor-friendly business climate. There he starts a new small high-cash business on paper, say a fashion shop or nightclub. He rings up lots of transactions and creates EUR 1.00 million in new profit. He pays taxes on that, at the flat rate of 19%, after a deductible of EUR 500,000 investment bonus (which cost him only EUR 2,500 in a large envelope).

He now has around EUR 900,000 of clean money, which he wires to his holding company in France, as an "Indefinite business loan." His French company invests that money in real estate on the Riviera. He does this for a couple of years, then closes his Slovak operation, and starts again in the Czech Republic.

I'm not an expert in international finance, and this is a simple scheme. Slovakia, incidentally, ended its flat tax rate in 2013, and is most definitely not run by crooks. A more elaborate model would use management service fees, patent and trademark licenses, not-for-profit holdings with an educational mission, multiple entities in different jurisdictions and so on. With a little care one could make a net loss every year on gross profits of billions of laundered money. Note clearly that I am *not* suggesting you do this. It is a theoretical exercise.

My point is to show that stopping the cash economy does nothing to reduce large-scale criminality and tax evasion. It just ensures the big banks will keep more of the cash flows involved. When the banks do get caught breaking those AML rules on *real* drug money, they are slapped on the wrist for getting caught, and told to behave. In 2011, "Wachovia, accused of laundering about $378 billion from Mexico

and facing U.S. criminal charges, got off by paying a $160 million fine," reported the El Paso Times[216].

Built for Terrorism

The September 11th attacks and the PATRIOT Act gave the Spider the tools to crack down on independent bankers. The first targets were the Hawala networks, a traditional Muslim system of money transfer based on trusted brokers. The Hawala networks transfer cash from US and Europe to conflict areas like Somalia, which was considered a hot bed of Islamic fundamentalism after the 1998 attacks on the American embassy in Nairobi, and Pakistan.

The correlation of the Hawala networks with conflict zones was enough to justify action against them. In 2001, after 9/11, the US came down hard on the al-Barakat group[217], calling them "the quartermasters of terror." TIME magazine shouted, "A Banking System Built for Terrorism"[218].

In 1991, Somalia saw the exodus of its dictator, the collapse of its formal economy, and a long civil war driven by clan rivalry and inflamed by interference from its larger neighbors Kenya and Ethiopia. The country suffered massive emigration, like Lebanon before it. The stuttering economy depended on groups like al-Barakat for banking and telecommunications and above all, Hawala money transfer. Even into 2013, $2 billion, more than a third of the country's GDP[219] came as remittances from diaspora communities around the world.

Claiming that al-Barakat financed the attacks on the twin towers and Pentagon, the Spider smashed the company, and hunted down its executives, worldwide. As Wikipedia relates, "several of the captives held in extrajudicial detention in the Guantanamo Bay detain-

216 http://www.elpasotimes.com/news/ci_21239235/drug-cash-fuels-money-laundering

217 http://en.wikipedia.org/wiki/Al-Barakat

218 http://content.time.com/time/world/article/0,8599,178227,00.html

219 http://www.aljazeera.com/indepth/opinion/2013/08/201385182737112984.html

ment camps in Cuba are held because Joint Task Force Guantanamo (JTF-GTMO) intelligence analysts asserted they had some kind of connection to al-Barakat."

After long investigation however, it turned out that al-Barakat was innocent of funding any kind of terrorism. The 9/11 Commission found no evidence of the claims against Al-Barakat. In August 2006, Al-Barakat was removed from the terror watchlist. It took until 2009[220] to free two Somalis, held for their ties to Al-Barakat, from Guantanamo Bay, and only in early 2012 was the case closed by the UN Security Council.

Millions of Somalis are still waiting for their frozen money back. As far as I know there was never an apology for this, or any kind of change of policy. The Hawala networks are still considered a "threat"[221] in official language, and the UK government implemented the European Union Payment Services Directive (a Europe-wide law) in 2013, forcing Hawala networks to register, or cease operations. Barclays Bank, the last bank to allow accounts to be used for Hawala work, closed them in October 2013[222].

Attack of the Regulators

Hunting down small independent bankers on trumped-up "financing terrorism" charges lost its charm when Guantanamo Bay got full. It's not clear there is any constitutional argument against creating virtual currencies, nor against accepting money from one person to hand over to another. Indeed, this has never been cited as an offense.

220 http://dandelionsalad.wordpress.com/2009/12/21/the-stories-of-the-two-somalis-freed-from-guantanamo-by-andy-worthington/

221 http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/13208.htm

222 http://allafrica.com/stories/201310070451.html

Rather, the offense is framed as "operating without a money transmitter's license." It is on this basis that the UK government is still cracking down on Hawala networks. The first major use of this tactic against a virtual currency was in 2009, against e-gold. In March 2013, the US Treasury Department's FinCEN (Financial Crimes Enforcement Network), issued these guidelines[223]:

> *FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.*

And, in that same document, FinCEN stated explicitly that: "administrators and exchangers of convertible virtual currencies are money transmitters."

Later in 2013, the government turned its attention to Liberty Reserve[224], a digital currency business based in Costa Rica. The Guardian reported[225] said, "Liberty Reserve appears to have played an important role in laundering the proceeds from the recent theft of some $45 million from two Middle Eastern banks. The complaint against one of the Dominican Republic gang members allegedly involved in the theft states that thousands of dollars' worth of stolen cash was depos-

223 http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

224 http://en.wikipedia.org/wiki/Liberty_Reserve

225 http://www.theguardian.com/world/2013/may/28/liberty-reserve-arthur-budovsky-arrested-spain

ited into two Liberty Reserve accounts via currency centres based in Siberia and Singapore."

As Wikipedia reports, "the indictment charges the seven principal employees, as well as Liberty Reserve itself, with money laundering and operating an unlicensed money transmitting business, and seeks $25 million in damages. The charges were leveled using a provision of the Patriot Act, since Liberty Reserve was not an American company."

Perhaps I'm just numbed, yet the theft of $45 million seems small peanuts when shutting down a network with a million users, handling over $6 billion since 2006. And the story of Dominican Republic gang members flying to Siberia and Singapore to deposit literally thousands (yes, thousands) of stolen dollars seems straight out of a poor Hollywood script. Way too much precise yet irrelevant detail. Not to mention extraditing foreign citizens for breaking US laws outside of the US. Has the world accepted the role of the US as global policeman, enforcing its own laws anywhere it choses?

Liberty Reserve allowed anyone to create an account without identifying themselves, hence the money laundering accusation. They held funds on behalf of others, hence the "money transmitting without a license" charges. However, I suspect the real reason they were taken down was simply because they refused to give the Spider access to their servers.

Does the Spider ask operators of underground virtual currency exchanges to cooperate? We won't know for sure unless there is a leak, though we do know that the owner of Lavabit[226], an encrypted email provider, shut down his service in August 2013 rather than "become complicit in crimes against the American people." It turned out[227] the FBI had been demanding secret keys from him, with a gag order to

226 http://lavabit.com/

227 http://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden

stop him talking about it. So it seems fair to assume that the Spider puts pressure on many firms, including US-based BitCoin exchanges.

FinCEN has stated that anyone buying or selling BitCoins for profit (even in tiny amounts[228]) will need a license. This includes BitCoin miners, who are key to the BitCoin network, since they process transactions. In May 2013, the largest BitCoin exchange, Mt. Gox, a Japanese business, had its US accounts seized by the Department of Homeland Security, another of the Spider's many arms, for operating without a money transmitter's license.

Getting the proper licenses in the US is complex. As Faisal Khan writes[229], "By varying estimates it will cost an organisation almost US$75 Million in security deposits/bonds and about a 18-24 month process before you are granted a license for each state." As well as state licenses (covering the whole country), you may also need a federal license.

Despite the cost and the uncertainty, several BitCoin exchanges are starting to get licenses. BitInstant claims to be licensed in 30 US states[230]. In Europe, Bitcoin-Central[231] is licensed in France, allowing it to operate across the European Union.

How will the Spider deal with BitCoin? It's a question that many who have invested in BitCoin think about, at 4 A.M. when they wish they were sleeping. Clearly the digital currency presents some real headaches to the Para-state. If it does emerge as a viable decentralized currency with sufficient mass, the whole fight against e-gold, Hawala networks, Liberty Reserve, and such, was for nothing. Yet if the currency is crushed too soon, we'll see the Dangerous Young Men effect. Cut down one Napster, and a dozen spring up in its place.

---

228 http://www.wired.co.uk/news/archive/2013-05/23/bitcoin-atm-money-laundering

229 http://payment-systems.quora.com/The-Money-Transmitter-License-Dilemma

230 http://bitcoinmagazine.com/bitinstant-we-have-money-transmitter-licenses-in-30-states

231 http://bitcoin-central.net

Better, the Spider calculates, to buy time and find a way to control BitCoin, and make a profit from it. BitCoin is a surprisingly strong model in some ways, yet it still has several vulnerabilities. It will depend on exchanges for converting BitCoin to other currencies until it gains (if it ever does) a sufficient internal market. BitCoin transactions — the blockchain — are essentially public, and it's been shown that you can tie transactions back to individual identities.

Lastly, and most importantly, the whole system depends on a distributed network of "miners," who recalculate transactions, and in the process generate new BitCoin. BitCoin depends on its miners to remain honest. If an attacker controls 51% or more of the miners, they can generate bogus transactions and crash the currency.

The cost of a so-called 51-percent attack is estimated at about $500 million[232], as I write this, the military budget of Slovenia or Cyprus. It's still well within reach of the Spider and even if the dangerous young men rallied in huge numbers, they might not be able to save BitCoin from a serious attack. I'd rate the chances of a 51-percent attack as "fairly likely" within the next 3-5 years. However it would probably be possible to counter such an attack by blacklisting offending machines.

What we will see instead is, I think, increasing persecution of BitCoin users, miners, and exchanges in the US, with the message that "BitCoin is favored by cybercriminals and money launderers." Perhaps some arrests to underscore the seriousness of the accusations. Then, tolerance of a few exchanges, allowing one or two to dominate the market and create a cartel. These will be the ones providing data live to the Spider, as the phone companies and large Web businesses do today. Finally, a series of attacks, from mild to shocking, on the currency when the critical number of black hat miners is reached.

If the BitCoin network survives the different attacks that seem inevitable — and I give it a 50-50 chance of surviving — the crypto currency will get a natural monopoly for on-line commerce. At a certain

232 https://www.resallex.com/bitcoin/brix

point buying or selling BitCoin for dollars or Euros will not be so important: people will simply hold and spend BitCoin. If the network does not survive the attack, the currency will die, and other crypto-currencies will take its place. Either way, the Spider will lose this particular fight, and the Para-state will eventually (it may take decades) find itself facing a truly independent financial system.

Licensed to Make a Killing

When I see sustained, multilateral action against systems as organic and valuable as Hawala and BitCoin, my first response is to slice up the official story and look for the lies. The second step is to look for the truth, outside the official tales. And it's almost always about money, profit, someone's private benefit.

While the independent money transfer industry was being closed down, other firms grew very large and profitable. One in particular has become a global leader. You will see the yellow and black "Western Union Money Transfer" signs in hundreds of locations in most cities. Western Union is an old firm, familiar with monopoly power. In 1987, having lost its monopoly over telecommunications, it entered a twenty-year restructuring that ended with a new Western Union emerging in 2006, focused on consumer-to-consumer money transfers.

It is simple to see the difference between a monopoly and a cartel in any given market. First, you look at prices. Second, you look for competitors. If the prices are higher than they should be, and there are competitors, you see a cartel. If the prices are higher than they should be, and there are no competitors, you see a monopoly.

Let's look at the cost of sending money using Western Union. Ask.com tells us[233], "The cost of sending money from New York to London in UK cost 13.32 pounds for every 100 pounds." When you send money to a developing country, the cost is higher. You also pay in expensive "0% commission!" currency conversions, so the real cost can

233 http://www.ask.com/question/how-much-is-the-western-union-fee

be as much as 20%. This is extraordinary, given that no money is actually being sent anywhere. It's just electronic messages. The biggest cost is probably the paper form one has to fill in, and the front office that types it in, and takes a copy of your ID "for security purposes."

Now let's look at competitors. The largest competitor to Western Union is MoneyGram International, one tenth the size. There is a mathematical "power law" called Zipf's Law[234] that models the distribution in natural systems such as free markets, earthquakes, cities in a country, and words in a language. Yes, all these follow the same rules of distribution. Normally, you'd expect the largest firm to be twice the size of its next competitor, three times the size of the one after, and so on.

The data shows that Western Union, too large and too costly, has a monopoly over the money transfer market. In 2011 alone, Western Union added 7,500 points of sale by buying the Angelo Costa group for $200 million. It then bought Travelex's payments division[235] for $976 million in cash, giving it another 950 stores and 450 ATMs in Europe. Then it bought Finint[236], giving it 10,000 locations across Europe. Western Union did not say how much they spent on this acquisition.

And MoneyGram, though it appears to be a competitor to Western Union, is according to Wikipedia[237] in fact operated by Western Union since 2006. I could find no other reference for this so it may be more or less accurate.

Usually it's the job of the government to stop firms getting monopoly positions or creating cartels. They do this by blocking the merger or acquisition of competitors by the market leader. However when a

234 http://en.wikipedia.org/wiki/Zipf's_law

235 http://www.bloomberg.com/news/2011-07-05/western-union-to-buy-travelex-payments-unit-for-976-million.html

236 http://ir.westernunion.com/News/Press-Releases/Press-Release-Details/2011/Western-Union-Completes-Acquisition-of-Finint-Srl/default.aspx

237 http://en.wikipedia.org/wiki/MoneyGram

government does nothing, monopolies can form quite rapidly and smoothly. The market sees nothing except the suspension of cost gravity.

One wonders why and how Western Union was given a blank check to gobble up its competitors and create a global monopoly. One might also wonder if the heavy handed crackdowns on informal — and cheap — money transfer systems is connected to WU's growth. According to the American Bar Association[238], the 2000-08 Bush administration filed the lowest number of anti-trust cases per year of any administration since 1948 (their earliest figures).

However, WU's rise to power seems more crispy, more tasty. It smells interesting, and not just because it's essentially all about money. Remember that part about copying your ID every time you send money? I think what WU is building is something akin to a Facebook for the Undocumented.

The money transfer business is a global map of every brown or black-skinned diaspora migrant who has money and sends it home. A map of who they talk to, who they trust, overseas. A database of senders and receivers of lucre, heads of families, chiefs of villages, people of influence of many colors. This is, I suspect, what Western Union is compiling, because it's possible, and it's part of the Spider's "know everything about everyone" obsession.

Is it accurate and prudent to suggest that Western Union is working hand-in-hairy-leg with the Spider? This is something I'd have to ask my lawyers. However, in his book "The One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11," Ron Suskind writes about a meeting between the FBI, CIA, and Western Union at CIA headquarters[239]:

> *[FBI official] Lormel talked about what a good friend Western Union has been since 9/11. Nervous Phil [a CIA pseudonym]*

238 http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/Dec09_Godek12_17f.authcheckdam.pdf

239 http://cryptome.info/western-union.htm

talked a bit about what might be done going forward. Western Union had twelve thousand offices across the globe, thirteen hundred in Pakistan alone. There was no country more important in battling the terrorists.

Everyone nodded, a show of consensus, until one of the Western Union executives had something to say. He looked at Tenet. "Here's my concern," he said. "If it seems that Western Union is a global front for the CIA, we'll go out of business." Tenet leaned forward in his chair and dropped his ace. "I know we're asking a lot," he said. "But this country is in a fight for its survival. What I'm asking is that you and your company be patriots." After that, it was all about logistics.

The War on the Middle

The devastation of the US middle class, and indeed the global middle class, isn't a failure of the system. Rather, it is one of the Para-state's great successes. I explained in "Faceless Societies" how the Bandits don't just compete with the Bakers, they actively attack them.

Extraction economies, such as the ones that runs mineral exporters like Congo-Kinshasa, Australia, the Gulf States, Nigeria, Equatorial Guinea, Russia, and increasingly, the US, don't just dislike representative government with its rules and social structures and costs. They deliberately tear it down, and replace it with compliant sockpuppets to rubber-stamp the mining and oil concessions.

In some countries this war on the middle takes the most vicious, violent form. It is my contention that the worst wars in Africa — such as Sierra Leone, Congo-Kinshasa, Angola, Sudan — were not ethnic or religious in nature, they are purely political. Worse, they were not about factions fighting for control. They were in most cases funded and launched with the express purpose of *destruction*, war for its own sake. It is the principle of "poverty on purpose," taken to its extreme conclusion. Bandits intent on stealing minerals by the truckload can

make much higher profits when there are wars and slave labor and no export controls, taxes, or paperwork.

Extraction economies are one case. More broadly, the Para-state faces the persistent threat of a general revolt against the extreme concentration of power and money. One of its core priorities is to make sure this does not happen.

Take for instance the French Revolution. Like every revolution, it wasn't planned, financed, and executed by angry mobs of laborers. It was pushed by the wealthy urban middle classes, who were denied a say in the running of the country. They allied themselves with the peasants to decapitate the royalty and create a republic. No middle class, no revolution. The poor do not revolt. They have too much to lose.

I think the attacks on the US middle class are blatant. We already discussed "mad mob" narratives such the reduction of politics to tribal grandstanding; the hype of emotional issues like marriage equality and abortion; the tight focus of the media on stories that do not matter, with silence on real issues. These all conspire to make society collectively stupider. It is the theory of cults, applied nationwide.

However, there are also deeper shifts in society that will take decades to recover from. The war on drugs is perhaps the worst case.

The War of Drugs

In the name of public health, drug policy has allowed mass incarceration of the poorest men, pumped up the prison system into a new form of slavery, funded the militarization of the police forces, corrupted law enforcement, and turned recreational drug users into criminals on demand, living in constant fear of arrest. The damage on US society is broad and deep, and it is damage done by bad laws, not damage done by drugs as such.

And in Central and South America, the drug war is burning democracy alive, just as the continent is recovering from decades of genocid-

al right-wing dictatorships installed, funded, and aided by the US. It is a classic, tragic war on the middle classes by an extraction economy.

One might claim that the demand for drugs is so strong that the flow cannot be stopped. However the price of drugs "has dropped relentlessly over the past two decades," according to the Economist[240]. That is a sign of strong supply, not strong demand.

The drug cartels are more powerful and destructive than ever, yet the Spider does not attack them. Drug money slushes around our financial system, yet the FBI does not arrest those accepting it. US drones can strike fear around the world, yet not haciendas across the border.

The US State Department documents[241] the eradication of opium production under the Taliban, down to 8,000 hectares in 2001 from 91,000 hectares in 1999. And then, the explosive rise to 165,000 hectares by 2006[242], after the US-led invasion ended the Taliban's prohibition.

The Spider clearly does not consider drug lords as dangerous as hackers. It seems implausible that if it can track Tor websites like Silk Road, it cannot track billions of dollars of money flowing through the world's bank accounts. After all, the Spider is so close to the world's financial system that it treats an attack on www.paypal.com like an attack on www.cia.gov.

It seems credulous to accept that we're losing the war on drugs by accident. We sent armies around the world to hunt down a few men in a cave, after 3,000 people died on September 11th. Overdoses from dangerous drugs like cocaine were the leading cause of death in the US in 2010, killing 38,329 people[243]. Drugs are as dangerous as they are profitable.

---

240 http://www.economist.com/blogs/dailychart/2011/06/uns-world-drug-report

241 http://2001-2009.state.gov/p/inl/rls/rpt/90561.htm

242 http://www.state.gov/cms_images/opium_poppy1986_2006.jpg

243 http://www.hightimes.com/read/drug-overdoses-number-one-cause-death-us-2010

The Afghan opium trade reached $70 billion[244] by 2013. The street value of that heroin is orders of magnitude higher. Afghanistan is only one of many zones of drug production. The volume of money that the drug trade represents is truly astounding.

I'm sure we'll see action by the DEA, aided by NSA wiretaps, against drug dealers, just as we do see action by the FBI against money transmitters. However the simplest explanation for the situation with is that the Para-state sees illegal drugs as one of its main business lines, and a useful tool to keep social resistance low. And the Spider loves those billions of Dollars of untraceable money that it can use to fund its most secret operations.

The War on Health

The other drugs trade is, of course, the health care system, which is also highly lucrative, and yet brings the US between Bahrain and Cuba in terms of life expectancy. The failure of the US to build a working health care system isn't due to lack of examples elsewhere. Aging populations are putting a strain on Europe's "socialist" models, yet despite that, they work.

Expensive, substandard health care is compounded by cheap, substandard food. Sugar mixed with white fat and white flour is not food. It is rather closer to an addictive drug, and it has a lifelong impact on health. The "Fat Americans" caricature becomes macabre when you realize that sugar obesity is a form of physical and psychological restraint.

The War on Wealth

Credit cards, reverse mortgages, predatory lending, student loans... the financial industry has made and is still making a killing by asset-stripping the US middle classes. An impoverished middle class is no threat to, and indeed, becomes fertile ground for, authoritarian ex-

244 http://www.khaama.com/annual-value-of-afghan-opium-trade-reach-70-billion-206

tremism. I think the lack of resistance to the growth of the US police state is directly due to the evisceration of the middle classes' wealth.

One doesn't need to invoke a deliberate strategy here: it's just convenient, and very profitable to at the same time prey on the middle classes while keeping them weak. Political conflict, even when it has consistent long term outcomes, does not require conspiracy of thought, just conspiracy of interests.

Wrapping Up

In this chapter I described some of the battles in a war of occupation by the Spider on digital society, and by extension, on broader society. Whereas digital society sees the Internet as its native territory, the Spider sees it as a principle tool for global social control. Who controls the medium controls the message.

I've not spent enough time on OWS, police budgets, financial crimes, or Anonymous. There are too many stories to tell. Search for them, and you will find them in masses. What we are witnessing is, I believe, an alignment of force to prevent, at all costs, the digital revolution from sparking off a real global revolt against the Para-state. What happens next is anyone's guess. In the next and final chapter of this book, I'll tell you mine.

Chapter 8. The Reveal

If you can't find the sucker at the table, you're it. — poker wisdom

There is no question that we are in an era of conflict between the haves — the Para-state — and the rest of the planet, with the Spider doing the footwork. What is new is not the conflict itself, which stretches back in history. What is new is its scale, and our recent ability to decrypt, document, and share knowledge about it. This is starting a slow yet profound shift in how we see the world. In this chapter I'll explore the conflict in more detail, especially in the real world, and the reveal.

One Planet, One Future

Zbigniew Brzezinski, National Security Advisor to President Jimmy Carter, wrote in his 1970 book "Between Two Ages,"

> *The technotronic era involves the gradual appearance of a more controlled society. Such a society would be dominated by an elite, unrestrained by traditional values. Soon it will be possible to assert almost continuous surveillance over every citizen and maintain up-to-date complete files containing even the most personal information about the citizen. These files will be subject to instantaneous retrieval by the authorities.*
>
> *Another threat, less overt but no less basic, confronts liberal democracy. More directly linked to the impact of technology, it involves the gradual appearance of a more controlled and directed society. Such a society would be dominated by an elite whose claim to political power would rest on allegedly superior scientific knowhow.*
>
> *Unhindered by the restraints of traditional liberal values, this*

elite would not hesitate to achieve its political ends by using the latest modern techniques for influencing public behavior and keeping society under close surveillance and control. Under such circumstances, the scientific and technological momentum of the country would not be reversed but would actually feed on the situation it exploits.

Persisting social crisis, the emergence of a charismatic personality, and the exploitation of mass media to obtain public confidence would be the steppingstones in the piecemeal transformation of the United States into a highly controlled society.

Will our children live in a post-industrial wasteland, where rich and poor live as two divided societies? Where food, water, privacy, and travel are rare luxuries, and where the digital infrastructure has become so pervasive and intrusive that every aspect of our lives is recorded, tracked, and modeled by the Para-state? Or will they live in a planet-wide meritocracy, where most of the old industrial economy has gone digital, where the old cities no longer exist except as leisure centers, and every human on earth except the mentally ill is on-line, all the time, everywhere?

It's a question only history will answer, and probably lie about, too. Perhaps history can give us some hints, though. We are an at times quarrelsome, violent, brutal, and highly destructive species. And we are also somehow gifted with the ability to make things better, given time. Every regime dreams of a thousand years of social control, and yet every regime collapses, as cost gravity steals the technological advantage it holds over its citizens.

Once Upon a Time in America

Cheap communications have changed our society more than any other of our inventions and it has removed more tyrants from power than any weapon. Let's take another step into the history books, back to May 1st, in 1844. Alfred Vail, working with Samuel Morse, was set-

ting up the first telegraph line, and on that day sent the world's first ever electronic message down the 24 miles of cable that were working, from Annapolis Junction to Washington D.C., to report the results of the Whig Party presidential nominations (Henry Clay won that nomination, and lost the subsequent election).

Just a decade later in 1855, the New York and Mississippi Valley Printing Telegraph Company and the New York & Western Union Telegraph Company merged to create Western Union. One assumes new-york-and-mississippi-valley-and-western-union-printing-telegraph-company.com was already taken by domain name squatters.

By 1900, Western Union operated a million miles of telegraph lines, and by 1945 it had an effective monopoly over the US market. As the New Yorker wrote[245], monopolies make spying easier. It is an easy and obvious trade: the government allows, by inaction or by intervention, a powerful telecommunications company to become dominant in a market through mergers and acquisitions. In return that company provides the government with surveillance.

The New Yorker explains how Western Union used its monopoly to serve those in power:

> *What we now call electronic privacy first became an issue in the eighteen-seventies, after Western Union, the earliest and, in some ways, the most terrifying of the communications monopolies, achieved dominion over the telegraph system. Western Union was accused of intercepting and reading its customers' telegraphs for both political and financial purposes (what's now considered insider trading).*
>
> *Western Union was a known ally of the Republican Party, but the Democrats of the day had no choice but to use its wires, which put them at a disadvantage; for example, Republicans won the contested election of 1876 thanks in part to an inter-*

245 http://www.newyorker.com/online/blogs/elements/2013/06/why-monopolies-make-spying-easier.html

cepted telegraph. The extent of Western Union's actions might never be entirely known, since in response to a congressional inquiry the company destroyed most of its relevant records.

It is quite visible how cost gravity drove communications down from an experiment for the wealthy to a mass market product so cheap even Western Union couldn't make profits from it. By 1980 its telegraph business was dying, and the old Western Union business was finally closed in 2006[246], after 151 years of operation. The name was, as we know, reused for a financial services company which today enjoys a government-sanctioned monopoly.

Curiously, Western Union's long telegraph monopoly seems to have had only a small impact on the size of communications networks. If cost gravity was operating fully, at 29% a year, and telegraph costs were in free-fall, there would have been 37M miles of telegraph by 1900. Instead, assuming Western Union had half the market, there were 2M miles. That is a factor of 16 over 55 years, which is not much, and a part of that can be accounted for by quality improvements.

I'm also not sure what to do with the random figure of 113 million kilometers[247] of fiber optic cable produced in 2010. A cable is a bundle of fibers, and the traffic rates are rather higher than Western Union's old stock. Has cost gravity been working?

One smoking gun pointing to a century and half of cost gravity being hijacked by telecoms monopolies back through AT&T and Western Union is the cost of the modern equivalent of a telegraph, the text message. Let's say the cost is one cent per message today. The purchasing price of $1 was 30 times greater in 1850 than it is today. If we apply cost gravity backwards, doubling that cost every two years, it would have cost over two million trillion dollars in 1850, allowing for that 30 times fall in the dollar.

---

246 http://en.wikipedia.org/wiki/Western_Union#The_end_of_telegrams

247 http://www.integer-research.com/2011/wire-cable/news/fiber-optic-cable-growth-continues-2012/

Clearly cost gravity stops working when monopolists run the table. Not only do we pay taxes to be spied on, we are also grossly overcharged for using the tapped lines.

Fairy Tales

Every expanding empire depends on a Narrative, a telling of the past, present, and future. A good Narrative has certain ingredients: a fearsome enemy, a dramatic disaster, a strong leader, sacrifice, and courage. It mixes a strong dose of national pride with paranoia and appeals to selfishness. The Narrative takes years to write, employing the finest propaganda specialists, and is then spun by careful retelling and fine-tuning, and repeated throughout the established media, over and over until it becomes as true as the day of the week, or the weather. It is more powerful than any army in keeping society acquiescent and under control.

The Narrative I was fed, growing up, told the story of a courageous free West battling the evil monsters of history — the Nazis — and facing off against the Soviets with their millions of armed soldiers waiting for any opportunity to smash our borders and seize our lands. At school, we were shown films that explained the Soviet threat. So many men, so many tanks, so many nuclear submarines, so many nuclear warheads, against the brave forces of NATO, all that kept us safe. The Narrative told us, be good consumers, vote for your chosen politician, and pray the nuclear war doesn't happen. And indeed more than once, the world came close to nuclear disaster. Three minute warnings were a fact of life.

The Narrative embraces and eulogies "just wars," such as those against Argentina, Iraq and Afghanistan, and invests in violence against faceless foreigners, in the defense of hard-won freedoms. It tolerates the massive sale of weapons to murderous regimes to fight "extremism." It denies climate change as "fake science," and it refutes ecological disaster as "fear mongering." It praises technology, above all

as a reason to consume, for our Narrative treats consumption and greed as natural, healthy, even necessary.

The Narrative promotes extraction economies no matter where they want to dig, and praises mineral wealth as a holy thing, for otherwise our life of luxury would end. It is a Narrative where elections and politics make us prosperous, and where economics is the official state religion. It is a Narrative that can find new enemies easily, be they revolutionaries in Central America, Ayatollahs in Iran, old dictator friends turned new embarrassment, even mysterious networks of international terrorists guided by dead men in mountain caves.

Technically, it is quite simple to draft a working Narrative. Appeal to selfishness? Check. Sword of Damocles? Check. Appeal to authority? Check. Bogeyman? Check. Nationalist pride and xenophobia? Check. Demands for sacrifice? Check.

And it is quite simple to sell it to the public. You just need a unified media, that is, one run by a few firms rather than by thousands. When you have a fragmented media, it is hard to control what they say. So you gently encourage the larger media firms to merge, unhindered by regulatory interference. You step back, stop anti-trust proceedings, and let businesses naturally merge and acquire their way to monopoly.

Once your market is ready, you arrange a few meetings where you say something like, "We were wondering how patriotic you guys are. If your country needed you, would you step up?" Anyone stupid enough to say "What about the Constitution?" is immediately investigated by regulators and his business is broken, and he ends up divorced, bankrupt, and imprisoned for fraud. The next meeting is about roles and responsibilities. "How about we send a few of our people to help you research the news?"

And so we end up with military intelligence teams working inside the largest media companies, selecting the news stories, and spinning them to reinforce the Narrative. In May 2000, Dave McGowan repor-

ted how[248] Major Thomas Collins, of the U.S. Army Information Service acknowledged: "Psyops personnel, soldiers and officers, have been working in CNN's headquarters in Atlanta through our programme 'Training With Industry'. They worked as regular employees of CNN. Conceivably, they would have worked on stories during the Kosovo war. They helped in the production of news."

In 1976, a Congress report into the CIA's Operation Mockingbird[249] noted that:

> *The CIA currently maintains a network of several hundred foreign individuals around the world who provide intelligence for the CIA and at times attempt to influence opinion through the use of covert propaganda. These individuals provide the CIA with direct access to a large number of newspapers and periodicals, scores of press services and news agencies, radio and television stations, commercial book publishers, and other foreign media outlets.*

According to Alex Constantine, author of "Mockingbird: The Subversion Of The Free Press By The CIA", in the 1950s, "some 3,000 salaried and contract CIA employees were eventually engaged in propaganda efforts." Officially, the program was ended[250] in 1976 by incoming CIA Director George H. W. Bush.

Inserting teams into existing media companies is one strategy. Another is to create your own business intelligence groups from the ground up. This is how large firms promote legislation, by funding "industry round tables" and "researchers" who push a pre-agreed message. The Spider has undoubtedly invested in many businesses, from armaments to drugs, and media. It's both profitable and convenient.

---

248 http://www.davesweb.cnchost.com/cnn.htm

249 http://www.youtube.com/watch?v=cDCfTIapdso

250 http://en.wikipedia.org/wiki/Operation_Mockingbird

Take as example The Economist, a respected and influential newspaper that was, ironically founded at the height of the patent debate in Britain as an anti-patent free-trade voice. It has a division called the Economist Intelligence Unit[251], which used to be the Business International Corporation[252], a CIA front company. BIC coincidentally employed a young Barack Obama.

Though you can fool many people most of the time, there is always a significant section of society that questions the Narrative no matter how well constructed and often repeated. It's those typical 20-something rebels, the intellectuals who think they're smarter than everyone else. They question everything, organize meetings, and suddenly you have a left wing anarchist movement making waves. That is when you praise the foresight of the men who preceded you. They knew the Narrative would only work so far, and that for every carrot you need something harder. So you open that super classified file and read the page, and you dial that number.

The Story Teller's Hammer

> *Terrorism and violent robbery have become a fact of life for Belgium. A spate of bomb attacks, originally on NATO targets, but recently on banks and offices, have been carried out by the mysterious Fighting Communist Cells (Cellules Communiste Combattantes, or CCC). The supermarket raids, more notable for the loss of life than the loss of cash, and a recent attack when a post office van was blown up and two postal workers were killed, have as much puzzled as shocked the country. The unruffled way the police are searching for the bombers and killers has been strongly criticized. — Chicago Tribune, December 1995*[253]

251 http://en.wikipedia.org/wiki/Economist_Intelligence_Unit

252 http://en.wikipedia.org/wiki/Business_International_Corporation

253 http://articles.chicagotribune.com/1985-12-05/news/8503240246_1_death-sentence-supermarket-ccc

On 9 November 1985, three armed men in balaclavas walked into a supermarket in the small Flemish town of Aalst, and began shooting shoppers and staff. There was no obvious motive for the extreme violence. No lone gunman, no robbery gone bad. It was direct violence against ordinary people. Four died that day. Fifteen more armed attacks followed, on supermarkets and jewelers in the towns around Brussels. 28 people died, many more were injured.

Belgium went into a short state of shock and then emerged, enraged. One thing about this small country: it has been hit often enough by bullies to recognize the hand of deliberate violence. The Belgian press quickly pointed the finger at the security services themselves, and specifically named Belgian military intelligence and the US Defense Intelligence Agency (DIA). The accusations were oddly specific, naming two military intelligence groups, SDRA8 and SDRA6, which no-one had heard of before.

No hard evidence turned up. Whomever had leaked the information didn't come forward to confirm it. The Belgian public concluded, largely, that the attackers had come from one of the many barracks housing armed paramilitary police. Their motives? Presumably to create a climate of fear that justified more militarization. That backfired. Belgians demanded and got an end to autonomous armed police forces. The Belgian parliament reformed the federal police, and instituted monitoring of the secret services.

It is a stark lesson for the US and its police militarization program. It's one thing, dangerous in itself, to bring military-grade weaponry and training into civilian law enforcement. The real stupidity starts later, when you try to roll back the program, and those armed and trained men decide they don't agree with you.

It took years for the truth of SDRA8[254] to emerge. The 1992 BBC documentary[255], "Gladio" tells the story of "Secret armies, funded by the United States, trained by Britain, and left behind in post-war

254 http://en.wikipedia.org/wiki/Belgian_stay-behind_network

255 http://www.youtube.com/watch?v=j1fH3YpQciQ

Europe to fight the rise of communism," and "the story of how they turned against their own people." Operation Gladio[256] ran from at least 1951 until 1990, four decades long.

Swiss historian Daniele Ganser explains[257], in his book "NATO's Secret Armies," how Gladio was exposed by a single stubborn judge:

> *The scandal originally came to light in Italy in 1984 when an Italian judge Felice Casson reopened the case of a terrorist car bomb in Peteano in 1972 and uncovered a series of anomalies in the original investigation. The atrocity which had originally been blamed on the communist Red Brigades turned out to be, in fact, the work of a right wing organization called Ordine Nuovo.*
>
> *Following the discovery of an arms cache near Trieste in 1972 containing C4 explosives identical to that used in the Peteano attack, Casson's investigation revealed that the bombing in Peteano was the work of the military secret service SID (Servizio Informazioni Difesa) in conjunction with Ordine Nuovo. The intention had been to blame the bombing on the extreme left wing militant outfit, the Red Brigades. The right wing terrorist, Vincenzo Vinciguerra was arrested and charged and confessed to planting the bomb.*
>
> *Judge Casson's investigation also revealed that the Peteano bombing was the continuation of a series of bombings begun at Christmas 1969, the most well-known of which, on the Piazza Fontane in Milan, killed 16 and injured 80. The bombing campaign culminated on 2 August 1980 with a massive bomb in the waiting room of Bologna railway station which killed 85 and injured 200. It was one of the largest terrorist outrages on mainland Europe in modern times.*

256 http://en.wikipedia.org/wiki/Operation_Gladio

257 http://wikispooks.com/wiki/Operation_Gladio

In short, NATO funded and organized secret cells of armed men and women across Europe, who bombed, kidnapped, and murdered civilians, politicians, and even NATO themselves, in order to promote the myth of communist insurrection in Europe. The Baader-Meinhof Gang, Bende van Nijvel, Red Brigades, Red Army Faction, Action Directe, Black September, all were likely either infiltrated, helped, and steered by Gladio, or run by it.

I'd include the IRA except that there was apparently no Gladio activity in the UK. In Northern Ireland, it was MI5 that penetrated the IRA and then allowed their agents to run amok, even killing other MI5 agents to maintain their cover.

Italian judges like Casson are a rare breed: fearless men who had the independence and authority to fight the deep corruption of Italian politics and law enforcement by criminals including, it turned out, foreign military intelligence services. Italy was, after World War 2, one of the main battlegrounds in Europe, between the Spider and a left-leaning society.

In her article "A judges' revolution? Political corruption and the judiciary in Italy," Donatella della Porta explains that although Italian judges were historically allied with political parties, and complicit in corruption, this started to change in the 1970's:

> *In the 1970s and the 1980s, however, the voice of the left within the judiciary became increasingly audible. In the judicial system, the so-called pretori d'assalto often took anti-governmental stances on labour and environmental issues (Bruti Liberati 1996: 186). At the same time, especially in the fight against terrorism and the Mafia, the magistracy exercised a proactive power, and acted as a surrogate for a weak political will to take any action.*
>
> *The dedication of many judges, who often paid for their defence of Italian democracy with their lives, was contrasted with the collusion of a divided political class; public opinion endowed the magistracy with a form of direct legitimacy.*

Moreover an increasingly strong ésprit de corps was developing among the judges (Colombo 1997).

In the late 1980s and the 1990s, a growing institutional autonomy of the judiciary resulted in a weakening of the attitude of complicity of some judges with those political forces which had partly hindered the activities of the magistracy. A new generation of so-called giudici ragazzini (child-judges) — lacking any sense of deference towards political power, and conscious of the high levels of collusion between politicians and organised crime — began a series of investigations into administrative and political misconduct.

Judicial investigations into political corruption have increased in frequency and magnitude over the past few years, culminating in the recent political upheavals caused by the 'clean hands' investigations of corruption, producing what has been termed as a 'revolution by the judges'.

The rebel judges did not have an easy time: they were persecuted by politicians, by turns bribed and starved, had their careers broken, and sometimes died, for their dogged pursuit of high-ranking criminals. As della Porta writes, "One corrupt Sicilian politician, for example, 'invited judges or their wives to teach courses in specialist schools, offered consultancies to important members of the profession, attaching themselves to the professional and entrepreneurial circles of Catania and transforming corruption into the rule'."

It took decades to bring down Silvio Berlusconi, one of the most corrupt leaders of any European country in recent history. Nonetheless, it is a testament to the strength of human nature that in Italy, the honest majority finally succeeded in reigning in the bandits and kicking them off the seat of power.

NATO was created to protect us from the Soviet threat. Instead, it appears, it funded and trained armed cells to murder, kidnap, and bomb our European cities. These cells worked hand in glove with

right-wing extremists, criminals, US intelligence, and paramilitary police. They stopped only because they were discovered in the act by investigating judges who, against all the odds, defied their political masters. There were no apologies, no justifications given, no inquiries beyond the outraged national parliaments. And this program lasted at least 40 years.

Gladio is more than a working hypothesis. The Belgian Parliament website[258] notes, on its page, Commissions of Inquiry set up by the Federal Parliament[259], "1990 — Commission of inquiry tasked with the investigation of recent revelations over the existence in Belgium of a clandestine international intelligence network, known as "Gladio"".

There is something deeply unsettling about hearing stories like Gladio. It like hearing someone talking about your best friend plotting to harm you. It's disturbing to have your own judgment on matters of life and death questioned. If we are so wrong about someone or something, what else could we be wrong about? Who else is plotting to hurt us?

Gladio was barely reported in the mainstream media. As far as the Narrative goes, these events did not happen, and Gladio did not happen. However the mainstream media no longer has the monopoly it had in 1990, and truths do emerge. When they do, the effect can be shocking.

A Theory on Theories

Two friends are sitting in a bar, sipping their coffees and discussing politics, when suddenly there is a huge explosion outside that shatters the windows and rattles the whole building. They run to the door and watch a massive cloud of smoke rise some streets away, over the buildings. A few minutes later, the radio announces, "Anarchists have struck again, bombing the Ministry of Peace."

---

258 http://senate.be

259 http://www.senate.be/com/onderzoekscommissies_nl.html

The first man sits down, wipes the dust off his cup, and takes another sip. "Bloody anarchists," he says, "I hope they get them this time." His friend says, incredulously, "Anarchists? C'mon, that's the fifth bomb this month, and every time they parade some hapless idiot in front of the cameras to give his confession. I think the authorities are the ones placing the bombs so they can arrest dissidents."

The first man shakes his head violently, "That's crazy talk! You think the Government would blow up its own buildings? What are you, some crazy conspiracy theorist? Oh my god, don't you know *anything*? It's the anarchist underground, working for the enemy. You're not an anarchist are you, now?"

It can be hard to discuss science when society is going through a period of insanity. The cries of "heretic!" and burnings at the stake may be history, yet the same patterns of thought run through modern societies just as they did through medieval society. Searching for truth, in a theocracy, can lead to harsh punishments. Galileo Galilei, for insisting that the Earth turned around the Sun, was tried for heresy, forced to recant, and put under house arrest until his death.

When mysterious things happen — like car bombs in the street, or lights in the sky, or newborn goats with two heads — we all immediately seek an explanation. It's part of the human thought process, the need to understand. Indeed, when we cannot understand and process some major event, we become numb and slow.

We have two major and opposing strategies to deal with unacceptable mystery. These are: magical thinking, and evidence-based thinking, which we also call "science." Magical thinking starts with an grand explanation that appeals to emotion and self-interest, and then it collects support for that explanation.

Science on the other hand, formulates theories and then tries to break them with evidence, reproducible data, facts. Large theories are disassembled into smaller ones so each piece can be tested independently. A piece of theory that cannot be broken remains on the table. Those that break or cannot be reproduced are discarded and forgot-

ten. The pieces that survive are put together, like a puzzle, to form the simplest plausible whole.

Conspiracy theories are an essential tool for criminal investigation based on science, rather than magical thinking. When two people in a room plan a criminal act, that is a conspiracy. To formulate theories about conspiracies, test them against the evidence, and discard the ones that break is not crazy, or misguided, it is literally *the only way* to approach the truth.

When someone uses the term "conspiracy theorist" as an insult, it is precisely like a true believer shouting "Crazy scientist!" at Galileo Galilei. The clinging to magical explanations is rational, for it is much safer and cheaper to stay in line with a theocracy than to argue with it. When the Pope makes an infallible declaration from his seat of power, you either accept it, or you are ex-communicated, arrested, tortured, and worse.

Theocracies are power structures based on magical thinking. They are large cults that purposefully fill the minds of their vassals with nonsensical stories. Magical explanations don't just satisfy the lazy urge for a quick explanation. They actively hunt down and destroy logical answers, as theocracies actively hunt down and destroy science.

How do you recognize a theocracy? Sometimes it's easy, there is literally a big organization that calls itself "The Church," and which decides who runs the country. Other times, there is no official church. However, organized religion is primarily an exercise in mass communications. When you have a compliant media that repeats magical explanations from the people in charge, you have a theocracy.

Poisoning the Well

It is only through a science-based investigation that any crime can be understood. Science is hard work, with little reward except the truth itself, and it is easy to poison the well to make it hard or impossible for the scientific process to work. This is as true for criminal investigations as for any other form of science.

In a criminal investigation you collect physical evidence and statements from witnesses. You develop theories about the event, and you try to disprove these theories with evidence and statements. When you have broken all the theories except a few, you take the simplest theory as the best-fitting truth.

As a process it is delicate and fragile. Clearly when a crime has a political motive, there will be parties with a strong economic interest in promoting magical theories, and stopping proper investigation into the case. I'll list just some ways to interfere with the scientific process:

- The *schoolyard attack*, where the media calls the investigators rude names, appealing to the part of the population that enjoys thinking like teenagers.
- The *reputation attack*, where the media casts doubts on the investigator's motives, suggesting they have a hidden agenda, or are working for the enemy.
- The *credentials attack*, where the media cast doubts on the investigator's credentials, saying they are not true experts.
- The *thin ice attack*, where the media says that anyone questioning the official story line is provoking social instability.
- The *strawman attack*, where plausible yet fake evidence is secretly provided to investigators, who use it, and are then exposed as "gullible and unreliable" if not actually incompetent.
- The *evidence chain attack*, where critical evidence is destroyed, hidden, or tampered with.
- The *testimony attack*, where witnesses are coerced into changing their stories, are persecuted for leaking state secrets, or die in mysterious ways.
- The *insertion attack*, where evidence and witnesses appear from nowhere to support the official story.
- The *sexual deviancy attack*, where someone associated with the investigation, perhaps a key witness, is shown to be a "sexual deviant," thus relegating the entire investigation to the margins.

- The *rising bar attack*, where unattainably high standards of proof are demanded from investigators who propose alternate theories.
- The *revolving door attack*, where investigators who cast doubt on the official story are fired or moved to other work, while those who promote the official story are promoted.
- The *rubber hose attack*, where tenacious investigators are simply removed from the picture, by bribery, blackmail, or force.
- The *broken chair attack*, where official investigations are controlled by key individuals who ensure the outcome upholds the official theory.
- The *reductio ad absurdum*, where exaggerated "crazy" theories based on clearly flawed evidence and reasoning are widely promoted, to discredit plausible theories.
- The *crazy chaff attack*, where the public is overwhelmed by attractive and yet flawed theories, making it hard for valid investigators to gain any audience.
- The *cold trail attack*, where an official investigation is delayed until it is too late for evidence and witnesses to have survived the inevitable accidents.
- The *embrace and extinguish attack*, where an official investigation is started and then its findings are delayed for years, or indefinitely.
- The *denial-of-service attack*, where honest investigators are overwhelmed with other events and work, so are unable to focus on the event in question.

When an event is planned, rather than covered-up, other attacks on a proper investigation are possible, such as planting fake evidence trails in advance, framing patsies with circumstantial evidence, or moving corrupted individuals into key positions ahead of time.

Even a well conducted investigation, like the National Transportation Safety Board (NTSB) investigation into TWA flight 800[260], runs afoul of many problems. And in this investigation, fully 95% of the

260 http://en.wikipedia.org/wiki/TWA_Flight_800

exploded Boeing 747 was recovered and reassembled, and hundreds of witnesses were interviewed.

When we see a major crime that is not investigated properly, when we see evidence disappearing, or made to appear, or when we see unreliable confessions, then we must conclude that we are seeing a cover-up. That in itself is evidence, if not of direct responsibility, then at least of complicity. Airplane flight recorders — black boxes — are designed to survive smashing into a mountain or sink to the depths of the sea. When the black boxes disappear from crash sites, that is a sure sign of an evidence chain attack.

In 2013 the Belgian Federal Parliament re-opened the investigations into the Bende van Nijvel, this time investigating *the original investigators*, for failing to follow leads, losing vital evidence, and so on. This is how it should be.

Irregular Violence

States have always depended on irregular forces, privateers, and mercenaries to go places and do things their regular forces could not. Operation Gladio is only surprising if you are deaf and blind to history. The US, like other military powers, has funded, trained, and armed irregulars all over the world, from Vietnam to Afghanistan to Guatemala. Paramilitaries can do mayhem — assassinations, mass slaughters, bombings — that regular soldiers cannot.

The military love irregulars during conflicts because they can move rapidly, without waiting for approval, and operate with "plausible deniability," a term invented by the CIA. Further, they can infiltrate other groups, work behind enemy lines, and so on. It is only logical that military planners stock up on their paramilitary investments over long periods.

Official budgets can be used for private military contractors when there is an active conflict. In other cases, the money has to be untraceable, otherwise it would leave a chain of evidence. One source of black

or "ghost" money[261] is presumably drug trafficking. The secret armies, armed and bored, are natural partners for drug cartels. Still speculating, I'd guess much of the drug-related violence in Latin America originates with paramilitary secret armies originally built by the US.

Sometimes these armed men decide they actually enjoy the murder and money, and go off on a long killing spree. Look at Los Zetas, Algeria, the Interahamwe, Chechnya, Al Shabaab. Perhaps they or their high-level handlers decide the authorities need a lesson, to remember how important they (the privateers) are, so they organize a spectacular attack on the homeland.

And then the hapless authorities are taken by surprise, and in their endemic paranoia and chaos they fail to prevent the attacks. Maybe they even had lots of warning, they are still riddled with mistrust and deceit and they act like idiots. Maybe here and there, men stand back and let it happen because it serves their agendas.

However, after the attacks, the authorities rush collectively to clean up the evidence, blame the attacks on anti-social elements "who hate our way of life," and make arrests. They get confessions by torture, shield the real culprits from real inquiries, throw the patsies in prison, destroy any evidence they can, leave false trails, and they stop their own criminal investigators from finding the truth.

And then we get the insane conspiracy theories that say lizards from Mars did it using death rays. The theories are so stupid that when someone comes forward with real insights, they are tarred with the same brush. Except, there are no lizards on Mars. A spectacular terrorist attack just takes a few very well-trained, well-armed men with sophisticated technology and good connections.

This banal explanation fits the observable facts in most cases. It is a key insight, that terror attacks are relatively cheap, and require no massive, expensive conspiracy. Clearly some events take more planning than others. However, usually all it takes is to send a shipment of

261 https://www.google.com/search?q=cia+ghost+money

weapons and explosives to a danger zone, train a few dozen off-the-radar paramilitaries, and then keep funding going for long enough for those cells to become financially independent from the drug business.

One last point here. People will say, "a government would never murder its own citizens." Though it is a hopeful point of view, it is naive and flatly wrong. People in power consider themselves above natural laws. Mass death is perfectly acceptable when it comes to alcohol, tobacco, pollution, and poor health. Surely national security ranks higher than business. The deaths of hundreds, thousand, even millions, when justified by the needs of power, are "collateral damage." The only really solid rule is, "Don't get caught."

And what happens when some upstart politician discovers a program of secret armies and talks about shutting it down or worse, revealing it to the world? Well, he dies[262], and the program shifts to another agency, under another name.

Battlefield Earth

Since 2001, the mercenaries have their own formal businesses and are called "private military contractors," or PMCs. One of the most infamous in the second Iraq war was Blackwater[263], which renamed itself "Academi" after much bad publicity. Andrew Marshall reports that[264]:

> *The CIA hired Blackwater to aid in a secret assassination program which was hidden from Congress for seven years. These operations would be overseen by the CIA or Special Forces personnel. Blackwater has also been contracted to arm drones at secret bases in Afghanistan and Pakistan for Obama's assassination program, overseen by the CIA. The lines dividing the military, the CIA and Blackwater had become "blurred," as*

262 http://en.wikipedia.org/wiki/Andr%C3%A9_Cools

263 http://en.wikipedia.org/wiki/Academi

264 http://www.informationclearinghouse.info/article36648.htm

one former CIA official commented, "It became a very brotherly relationship... There was a feeling that Blackwater eventually became an extension of the agency."

In March of 2012, a Special Forces commander, Admiral William H. McRaven, developed plans to expand special operations units, making them "the force of choice" against "emerging threats" over the following decade. McRaven's Special Operations Command oversees more than 60,000 military personnel and civilians, saying in a draft paper circulated at the Pentagon that: "We are in a generational struggle... For the foreseeable future, the United States will have to deal with various manifestations of inflamed violent extremism. In order to conduct sustained operations around the globe, our special operations must adapt." McRaven stated that Special Forces were operating in over 71 countries around the world.

By September of 2013, the U.S. military had been involved in various activities in Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde Islands, Senegal, Seychelles, Togo, Tunisia, Uganda and Zambia, among others, constructing bases, undertaking "security cooperation engagements, training exercises, advisory deployments, special operations missions, and a growing logistics network.

The battlefield covers the whole world, and above all, the American homeland itself. The US is the keystone in the Para-state's power structure. It represents by far the richest food source for this parasitic political class. The US is wealthy due to three things: centuries of mass immigration, abundant natural resources, and a geography blessed with generous natural transport.

If it was not for the Para-state's predations, the US would be considerably more prosperous, easily affording first rate healthcare, education, transport to all its people, and a massively better technological infrastructure. As it is, other parts of the world have to show this

wealthiest of all nations how to build decent trains, schools, networks, health care.

If I was American I'd be embarrassed that for all my country's advantages, its main gifts to the world have been Coca-Cola, MTV and CNN, and countless nasty wars disguised as peace actions. However, as happened in Nazi Germany and Napoleon's France, the homeland is just the first conquest. After that comes the war of expansion.

Extraction economies — oil, narcotics, human trafficking — have always thrown acid at the face of society, because social structure and stability cut into profits. In October 2013, the US became the world's largest producer of oil[265], beating Russia and Saudi Arabia. The country is also the top market for drugs, and the leader in a modern form of human trafficking focused on poor men. As Robert Graham writes[266] in "Reflections of a Modern-day Slave,"

> *The (criminal) criminal justice system is a very well-oiled machine in which the powers that be regularly utilize their weapons of mass oppression in the concrete jungles all over America with military precision. Today, there are overseers lurking and prowling through inner-city streets like big game hunters with their sights fixed predominantly on minority men, ironically in a way equally as steadfast as slave poachers did in the days of old.*

The US has turned into the world's number one extraction economy. When I wrote about "Poverty on Purpose" with respect to sub-Saharan Africa, my explanation could also apply to Detroit, Oakland, East Greenbush, Harrisburg, Camden, Washington D.C, Chicago. The hollowing out of American's heartlands does not need to be deliberate, systematic policy. One simply stops investing in infrastruc-

265 http://online.wsj.com/news/articles/SB10001424052702303492504579111360245276476

266 http://www.publiceye.org/defendingjustice/overview/graham_slave.html

ture and education for the majority, and instead, invests in security for the minority.

Pandora's Box

It is no new conflict. What is new is the ripping away of the Emperor's clothes, the dropping of the mask, the loss of control over the Narrative. This particular empire depended on expensive mass communications as its technology of choice. Cost gravity has broken that monopoly by making it dirt cheap for anyone to publish content.

The Narrative told us that if we trusted our leaders, worked hard, spent our money on pretty things, and kept our heads down, they would keep us safe from the bad men trying to kill us. Over the years the bad men have morphed, from communists to Nazis back to communists, to Islamic extremists, and perhaps in another 80 years it will be the extremist vegetarians.

It is, we start to realize, a grand and yet obvious lie. Not only does our government not really succeed in stopping terror attacks, we see that it has invested, and still invests significantly, in groups that sooner or later end up committing terrorism. Confusion, chaos, or orchestration, it is hard to tell the difference sometimes.

Let me restate what should now be the working hypothesis for anyone studying this area: the Spider lets happen, or makes happen, terroristic events to maintain its ongoing Strategy of Tension. As backing evidence we have the Spider's decades-long investment in paramilitary networks abroad and at home, its involvement in the drug business, its easy breaking of constitutionality as it pleases.

Officially, Gladio was quietly disbanded in 1990. This reminds me of the compulsive liar who, when caught, promises to stop lying. It beggars belief that the Gladio networks stopped when they were unmasked. The liar does not stop lying, instead he becomes smarter about not being caught.

I spoke about Anders Breivik in "Faceless Societies". Norwegian lawyer Alexandra Bech Gjoerv headed an independent inquiry into the shootings. Here is how the BBC World Service reported the inquiry's findings[267]:

> *Among the most damaging of the report's conclusions is that a two-man local police team reached the lake shore at Utvika first, but chose to wait for better-trained colleagues rather than find a boat and cross to Utoeya themselves.*
>
> *The attack on the government complex in Oslo could have been prevented by effective implementation of security measures that had already been approved.*
>
> *A more rapid police operation to protect people on Utoeya Island was a realistic possibility and the gunman could have been stopped earlier on 22 July.*
>
> *Although it was clear that a terrorist attack had been carried out, the inquiry says no immediate nationwide alert was given, no roadblocks or observation posts were set up, no attempt was made to mobilise helicopters nor did the operation centre take up offers from neighboring police districts.*

There's a curious thing Breivik said, after he had finished his killing, and called the police to come and arrest him[268]: "My name is Commander Anders Breivik Behring in the Norwegian anti-communist resistance movement." From the translated Dagbladet article, "Breivik claimed that this movement was responsible for about 50 attacks in Europe since World War 2."

---

267 http://www.bbc.co.uk/news/world-europe-19241327

268 http://www.dagbladet.no/2012/04/01/nyheter/anders_behring_breivik/terrorangrepet/peter_mangs/utenriks/20928848/

Crooks and Liars

It is becoming acceptable to say, out loud, that our politicians are thoroughly corrupt. That the police exist to protect criminals from us, rather than to protect us from criminals. That conspiracies are real, not mythological, and that theories about crimes are not silly nonsense, they are an essential tool for establishing the truth. And, most dramatically, that the entire political establishment, left and right alike, our whole democratic system, is illegitimate.

Listen to Russel Brand speaking to the BBC's Jeremy Paxman[269]:

> ***Brand:*** *It's not that I'm not voting out of apathy. I'm not voting out of absolute indifference and weariness and exhaustion from the lies, treachery, deceit of the political class, that has been going on for generations now. And which has now reached fever pitch where you have a disenfranchised, disillusioned, despondent underclass that are not being represented by that political system, so voting for it is tacit complicity with that system and that's not something I'm offering up.*
>
> ***Paxman:*** *I'm not having a go at you because you want a revolution, many people want a revolution, but I'm asking you what it would be like.*
>
> ***Brand:*** *Well I think what it won't be like is a huge disparity between rich and poor where 300 Americans have the same amount of wealth as the 85 million poorest Americans, where there is an exploited and underserved underclass that are being continually ignored, where welfare is slashed while Cameron and Osbourne go to court to defend the rights of bankers to continue receiving their bonuses. That's all I'm saying.*

It is easy to dismiss Russel Brand as a cheap celebrity seeking fame by saying dangerous things. He dresses up like a Hollywood Jesus and used to be famous for his sexual conquests and drug use. However he

269 http://www.youtube.com/watch?v=3YR4CseY9pk

is articulate and precise in his accusations, and deals with his interviewers with such charming self-effacing brutality that he leaves them squirming in their seats.

Brand is one of a new generation of activists who are leading the collective thought process away from the Narrative and towards a more accurate view of reality that I call the Awakening. I fully expect him to suffer a suicide-accident-car crash, or accusations of deviant sexual crimes. He claims to be a stand-up comedian, yet in naming the political class as the enemy of society, he preaches revolution. And as I've written, when one person says "revolution," another reaches for his gun.

The Global Awakening

In cryptography, the hostile attacker is sometimes called "Mallory," which is cute until you understand that when security researchers across the world now say "Mallory," they are speaking of the Spider. There is no other threat that security researchers take more seriously.

With the loss of the Narrative comes a new realization, that we are a global society living under global occupation. The occupation may be invisible if you are wealthy, white, privileged. I certainly can't see it as I walk around Brussels, or drive around Dallas. As you go to your well-paid job and congratulate yourself on getting a good education and choosing the right parents, the notion of occupation is ridiculous.

Yet more and more of us are on the other side. We have at best part-time jobs that give us no security, pensions, or health-care. We are born in debt, and we die even poorer, while the mega-rich get richer. Our cities are desolate and abandoned through utter lack of interest from those with the power to make things better. Society is not just more divided than it should be, it is more divided than we can comprehend.

Perhaps, if you are a young white American, the reveal began when you saw the New York Police Department (NYPD) beating and arresting peaceful Occupy Wall Street protesters. Or, it was that phrase

"the one percent" that kept you awake at night. Perhaps it was years ago, when President Obama decided to keep Guantanamo Bay open, after all.

Perhaps the reveal crept in slowly, when you noticed the lack of criminal investigation into the misconduct of the Bush-Cheney regime. We saw two wars of aggression, lies at the highest level, torture, rendition, destruction of official records, and illegal spying on US citizens, and these were just the visible crimes. Yet not one single investigation. As I said, when we see major crimes not properly investigated, that is evidence at least of complicity.

Perhaps the reveal hit with a shock when you watched "Collateral Murder," the video of US forces[270] shooting civilians with 30mm ammunition from an Apache helicopter in Baghdad, leaked by Chelsea née Bradley Manning. Bullets over an inch across will make a large hole in any Narrative.

There are so many instances where the official story and the documented facts meet like strangers in the street, stare at each other in vague recognition, then shake their heads and go their separate ways. It's not just that there are a lot of lies. It's that there seems to be nothing *but* lies.

If you come from a poorer country like Congo-Kinshasa where the extraction economy rules, or one of the many countries where Western-sponsored violence has been a fact of life for centuries, nothing I've said will be a surprise. You will have seen the real face of occupation since you were young, whether your parents were part of the elite, or not.

Whenever the doubt started, it grew, and though you fought it, it kept growing until it filled all the space. We depend so much on the Narrative that questioning it, or hearing others question it is a painful, consuming experience. Observer columnist and academic John

270 http://en.wikipedia.org/wiki/July_12,_2007_Baghdad_airstrike

Naughton describes the emotion:[271] thus, "The minute you get into the JFK stuff, and the minute you sniff at the 9/11 stuff, you begin to lose the will to live."

Hopefully my tales of the Para-state and its Spider provides some backup, and a way to understand. The proper response to the loss of Narrative is not pessimism, it is optimism and exuberance. For only when we understand our past and our present, can we build our future. As long as we accept the Narrative, we are its thralls.

The Anti-Narrative Market

In "Spheres of Light" I described the market curve, which explains that society cannot learn as one body. Rather, new knowledge starts with ice breakers and pioneers, who teach it to early adopters, who in turn convince the mass market, then the late adopters, and finally the skeptics.

When we look at the Awakening, we see a process of cult deprogramming. It is a process of switching from magical thinking to evidence-based thinking. The shift is painful, stressful, and takes time, perhaps even years.

Some people naturally resist lies. Others need the lies explained, carefully, and over time. Yet others will cling to comfortable lies over difficult truths. All the while, as people search for the truth of things, they are targeted with exaggerated conspiracy theories that make any discussion difficult.

What we have is the development of an "anti-Narrative," a set of explanations and exercises that allow us to de-program ourselves, and others. Much of my book has been the development of anti-Narratives: the explanation of on-line communities, of how cults operate, of the spy state, of the Para-state and the Spider, and so on.

271 http://www.bbc.co.uk/news/uk-politics-24650841

The anti-Narratives emerge most powerfully from the pioneers in this collective de-programming exercise, the ice-breakers who, for diverse reasons, are prepared to go into incredibly hostile environments with nothing more than their self-faith to keep them going:

- It all begins with the whistle blowers, particularly those who can leak substantive documentation rather than personal stories and hearsay. Chelsea née Bradley Manning and Edward Snowden are the two main figures here, heroes in a real sense. Other whistle blowers of note are Annie Machon, Gareth Williams, Russel Tice, Jeffrey Sterling, Stephen Jin-Woo Kim, Jesselyn Radack, Thomas Drake, Daniel Ellsberg, and William Binney.
- We then have the independent media who are willing to report these documents, at personal risk. There is Julian Assange, building wikileaks.org around Manning's leaks, and Glenn Greenwald and Laura Poitras, reporting in the Guardian on Edward Snowden's leaks. Again, heroic figures who have changed the course of history.
- We see academics like Dr Daniele Ganser, who know their history and are immune to this particular Narrative because they have seen so many like it. They look at events over the last twenty years and they see continuation of old patterns.
- We have anti-patent and anti-copyright "extremists", like the Pirate Parties, the FFII (in part), the Pirate Bay and the many, many who took risks to share music and movies with other people. They know the law is unjust and wrong, and they have been providing elements of an anti-Narrative for years.

These are the ice breakers, whose message is ignored, mocked, and rejected until it swells to a point where it can't be brushed aside as hysterical, crazy nonsense. Any single thread or event is irrelevant. There is more than enough material to write a compelling anti-Narrative that fits the facts and cannot be broken. And it's this anti-Narrative that the early adopters take, and spread to the wider world. I consider the early adopters to be:

- Other independent journalists, who find themselves flooded by intensely interesting stories that the mainstream press will not touch. It is irresistible, to print these stories.
- Technologists, particularly privacy and security advocates, and smaller firms, who understand the importance of Snowden's leaks about the Spider, and who find the conclusions extremely worrying.
- On-line communities, who long ago developed a sharp taste for truths. Despite wide infiltration by the Spider, the Narrative died long ago in most on-line communities, as did conventional religions, cults, partisan politics, and other belief systems.
- Criminologists and forensic scientists who study specific events and find that the data disproves the official explanations; they then ask how that could be, and it leads them to larger questions.
- Environmental activists, who have always seen the Narrative and its glorification of extraction economies, war, and consumption, as their biggest problem and the main threat to human survival.
- The twenty-somethings, who are naturally distrustful of anything authority says, and have historically always embraced revolutionary principles, at least until their first job and car loan.
- Celebrities like Russel Brand, who need fresh material to stay relevant, so seek out new thought trends and emerging truths. Evangelists in any field depend on the latest and greatest to share with their followers.

Among the pioneers and early adopters I also have to include the billions of people around the world who have always seen the West as

a corrupt police state, and westerners as naive, complicit, and intellectually lazy. On behalf of the privileged white minority, I'm really, truly sorry we didn't realize what was going on so much sooner. To be honest, we still don't know what's going on, we are just becoming aware of the depth of the lies.

Then we have the mass market, which is more about industry than individuals. Particularly, the technology industry. Large firms have to play the Spider's game to stay in business. And yet if their clients lose confidence, they can pack up and leave overnight, as MySpace proved. They desperately need to retain their street credibility.

Large technology firms are stuck between a rock and a hard place, and I'm curious to see where they land. My guess is that there will be a break, with some firms coming down hard on the side of privacy and constitutionality, and other firms becoming closer allies with the Spider. It is one place where popular opinion can make a serious difference.

The late adopters are the monopolists like AT&T, Comcast, and Western Union, the oil companies, the financial industry, and the security industry, who depend on the Spider for their own safety. If these firms lose their gold club member status, they are broken up like old trash and sold off in pieces.

Where's the Steel?

In this book I've skimmed over many topics. I'm not a journalist, nor a historian, and I have no credentials except my words. Credentials — that lazy inheritance of trust from other people — are somewhat quaint in the on-line world. What we say can matter, who we are does not. Only one thing really matters, and that is the knowledge of truth, which we arrive at together.

I've tied to provide you with tools and models to help you understand the world, and find truth in it. Look for cults, small and large, and you will find lies and propaganda. Look for well-organized collective intelligences and you will find truths.

My children will be astonished, when they grow up and read this, to learn that in 2013, some truths were still too difficult to say out loud. Here is one example: I think the evidence shows that the major terror attacks in New York, Madrid, and London were organized and executed by the military intelligences of one nation or another. That the Strategy of Tension has been hard at work, and spectacularly successful. That the War on Drugs, and the War on Terror, rather than being miserable failures, achieved all their goals, and more: profit, power, and social control.

This is what I believe to be true, despite a decade of searching for other explanations, and it scares me to write it, and publish that, under my own name. I've seen the expressions of horror and pity on my friends' and family's faces when I explain this, which is not often. However, our best stab at the truth is all we have. It is our only shield and our only sword. When a truth is difficult to repeat, that makes it all the more important. Truths do not attack democracy, lies do.

To solve a large jigsaw puzzle, you start by finding the corners, pieces you can at least fix, while the rest is still chaos. To solve the large puzzle of what happened on September 11, start with one single piece: the neat free-fall collapse of the steel skyscraper called WTC 7 due to "office fires".

All the steel from WTC 7 was removed and recycled before investigators could examine it. All except one lonely piece, corroded and mangled. It took seven years for NIST to produce a self-contradicting report on WTC 7, based on paper arguments and computer models. In 2013 we learned that this same NIST had worked with the NSA to deliberately weaken international security standards.

Consider by comparison, TWA flight 800, where investigators pulled thousands of pieces of the exploded 747 from the sea, and then reassembled those into a 95% complete plane. If an important person in perfect health dies suddenly, in extraordinary circumstances, and the authorities cremate the body rapidly, against the wishes of the family, and without allowing an autopsy, that would be a conspiracy.

Big catastrophes demand big investigations. The destruction of the entire body of evidence, and the non-investigation of the WTC 7 collapse was a conspiracy. If we cannot investigate the events themselves, as the evidence was destroyed, then we must investigate the investigators for their crimes.

And then, what? When we have done our research and accepted that the official conspiracy theory was wrong enough to need a cover-up, that we were lied to repeatedly, what then?

David Chandler frames it eloquently[272]:

> *9/11 did not just happen. 9/11 was a premeditated shock and awe event that was instrumental in a larger plan. It allowed the administration to immobilize the population through fear and manipulate their outrage displaced toward the designated enemy.*
>
> *9/11 provided cover for a protracted attack on our democratic values and an orgy of outrageous national behavior that defined the entire Bush administration, much of which continues today.*
>
> *9/11 brought us the fiction of "preemptive" wars as a fig leaf for naked military aggression, the fiction of "illegal enemy combatants," to pretend the Geneva Conventions did not apply, and the fiction of "enhanced interrogation" as though that were any different from torture pure and simple.*
>
> *It brought us routine drone assassinations, the expansion of secrecy, the unleashing of the NSA to conduct universal surveillance, the destruction of nearly every one of our civil liberties, attacks on journalism and the murder of journalists, paranoid fear of immigrants in general and Arabs in particular, and the demonization of Islam as a uniquely violent religion. This list is far from complete.*

272 http://911blogger.com/news/2013-10-30/911-so-what

Once people become conscious of the fact that 9/11 was a lie, how can they channel their response? Their essential response must be to demand our democracy back. This can take a thousand forms. We must call for an end to the war on terror, which is in reality an endless reign of terror.

We must call for the end of drone assassinations. We must work to end the death-grip of the military industrial complex on our society. We must work to end the dominance of the fossil fuel industry over our government.

We must work to end economic polarization of the nation and the influence of money on politics. All of these, and many more areas of potential activism, are responses to the larger crimes against democracy that were launched on 9/11.

All of these can be energized by people who have become conscious of the truth of 9/11. Consciousness of the truth, is empowering. It changes who we are and how we understand and interact with the world. As we raise consciousness of the truth we incrementally change the social and political landscape. That is why we must continue to speak out.

Reading this, I see two possible futures. One is indeed the restoration of democracy, by wide political activism and careful, incremental dismantling of the Spider and Para-state. Perhaps US society, divided and weak, cannot do this by itself, and yet with help from Europe and the rest of the world, it can.

Realistically, it seems naive and over-optimistic to expect the Spider and Para-state to self-destruct simply because that is what everyone demands. We are talking about a large, powerful, and utterly ruthless bandit gang. Of course the creation of a police state is far easier when people are unaware. Yet once the police state is in place — and it is in place — does it actually matter what people know or think? There are so many ways to put down a popular revolution.

The Third Front

There are three main fronts in the undeclared world war I've described. These are the War on Drugs, the War on Terror, and the new War on the Internet. Let's take these individually and look at them from two sides. First, from the conventional perspective of the Narrative, and secondly from the perspective of the Awakening.

The War on Drugs, conventionally, consists of dark-skinned criminals who want to poison our youth with illegal drugs. Despite brave, endless police action against these violent men, the policy regretfully seems to be not working very well. Still, legalization would be like giving up. We will beef up our law enforcement efforts, bring in the army if necessary, and we will persevere!

In reality, the War on Drugs has been extremely convenient for the Spider, and profitable for the Para-state. It generates boat loads of cash, which it can use to buy influence and muscle without the troublesome paperwork of official funding. It is a ghost tax on the US domestic market. Drug related violence overseas makes good cover for Spider covert operations, infiltration of left-leaning governments, assassinations, and so on. Drug cartels make natural partners for the secret armies, since both treat the common citizenry as fair game. And the escalating violence, real or not, allows the Spider to infiltrate domestic law enforcement, militarizing the police across the US.

The War on Terror, conventionally, consists of dark-skinned extremists who want to destroy our way of life. Despite brave, endless police actions against these foreigners, the policy regretfully seems not to be working very well. Still, we cannot abandon such a serious threat! We will beef up our intelligence services, send in more drones, and even if this war lasts forever, we will persevere!

In reality, the War on Terror has also been extremely convenient and profitable for the Spider and the Para-state. It allowed the PATRIOT Act to slide through Congress. It gave the Spider unlimited space to consolidate its diverse agencies, and power to do what it

pleased, across the globe, in the name of "security." It ended the concepts of constitutionality, civil liberties, privacy, justice, due process. It legitimized the old practice of secret armies, and created havoc in the Middle East that drew all attention away from the ongoing eradication of Palestine.

Finally, the War on the Internet, which for a change makes no implied appeal to racism. Conventionally, a generation of young 20-something anarchist pirates have been stealing our cultural treasures, collecting kiddie porn, publishing plans for nuclear bombs, wreaking havoc on honest businesses, and leaking state secrets.

To stop these dangerous pirates, hackers, drug dealers, and cyberfreaks we need firm action, international agreements like ACTA[273] and the Stop Online Piracy Act (SOPA), which regretfully must remain secret for national security reasons. Sadly, this war will probably last forever. We will of course persevere, etc. etc.

In reality, copyright is a stalking horse for a fight to control and reign in the largest communications network in human history. Control the Internet and you control the future. We'll same the same patterns in the third front that we saw in the other two:

- A gradient of deniability that stretches from official operations, to private contractors, to secret armies, through to criminals.
- The building up of clusters of mercenary spy companies specializing in on-line terrorism: denial of service attacks on websites, identity thefts, evidence planting, computer intrusions, malware, and so on.
- The criminalization of on-line activists as "domestic terrorists," and their persecution, monitoring, infiltration, and arrest on constructed charges.
- The grooming and conditioning of the majority population to accept surveillance, by television "reality" shows, and by social networks like Facebook.

273 https://www.google.com/search?q=acta

- The promotion of monopolies that make it cheaper for the Spider to spy, combined with the threats against firms that do not collaborate.
- Large, significant attacks on civilian infrastructure, such as electricity networks or transport or payments, which will be blamed on domestic cyber-terrorists, and used to justify new powers to regulate the Internet.
- Many smaller attacks on businesses and individuals and homes to maintain the climate of fear. As with larger attacks, there will no proper criminal investigation.
- The criminalization of specific technologies, such as Tor and perhaps BitCoin, due to their use to support terroristic actions.
- Internet disconnections will be used as punishment for individuals who use banned technologies or visit banned websites.
- Pioneers in privacy and security will increasingly be given special attention by the Spider, and picked up for unrelated offenses, real or contrived. Along with independent journalists and whistle blowers, being a privacy advocate will become a dangerous profession.
- US-based cloud services, or cloud services with US customers, will be regulated in terms of the material they can host, and politically sensitive websites and forums will be censored. Foreign cloud services that host offending material will be attacked.
- Law enforcement will depend more and more on parallel construction — that is, evidence gathered through illegal surveillance and then "washed" to appear to come from legitimate sources — to find a crime to fit any suspect.
- Wikipedia, YouTube, and Amazon will be subject to various attacks that seek to remove politically unacceptable content as part of a strategy to "clean up" the Internet.

Little of this will work, though it will be a long fight. The Para-state has unlimited money, guns, and political power. The Internet has unlimited brains. Neither side can really beat the other.

Occupation Costs

In the world I grew up in, and if you're over 35 or so you may remember this world, South Africans still lived under Apartheid. That was a system of laws introduced by the National Party in 1948 to prevent any loss of power by the ruling white elite. South Africa was a society divided into white rich against brown and black poor. The land was governed by military power used against civilians, by torture, murder, and secret arrests. The free press was smashed, and political dissent quashed. Black South Africans were first deprived of their vote, and then of their citizenship and lands.

South Africa's Narrative used to be, for whites, "the black man wants to kill you and rape your wife and daughters, so we will move him far away from you, and make you safe," which was simple and effective. The quite different Narrative for blacks was, "behave and you may get a work permit. Resist, and your family will starve."

In South Africa there was no revolution, though, as there was in neighboring Rhodesia that became Zimbabwe. The South African regime was simply too powerful to be toppled by force. There was instead a long, determined struggle for freedom and equality that became increasingly well organized, militant, and supported by the international community.

And in the end, after decades of decrying the holocaust that would follow any transfer of power, the Boers lost control of their Narrative, and white South Africans, particularly the business community, experienced an Awakening. They realized that their vision of a thousand years of white rule was a lie. It was bad for business, and it was unpleasant both on the streets, and in global terms.

President Frederik Willem de Klerk released Nelson Mandela from 27 years of prison and found a willing negotiation partner. In 1994,

after years of violence and terrorism that turned out to be largely sponsored by the state security services themselves, negotiated multiracial elections swept the African National Congress (ANC) into office. Many whites left the country, bitter, and afraid of a retribution that never came.

Instead, incredibly, instead of a witch hunt and trials, there was a Truth and Reconciliation Commission (TRC), where victims could speak of their experiences, and torturers and murderers could speak of their crimes, and ask for amnesty. The TRC was widely criticized, for allowing criminals to escape justice, for not giving victims adequate time in court, even for being a "circus" in the words of former president P. W. Botha. Yet the TRC did largely work, creating a non-violent path from past to future.

South Africa is not an easy place to live: incomes are low and costs are high. It remains far from Europe and major markets. It has a reputation for violence that is perhaps exaggerated. The ANC turned out to be corruptible, like any government. The economy suffers from unemployment. Yet South African businesses, unleashed, have become giants across Africa and globally. In 2000, its GDP was $133B[274]. In 2015 it is forecast to hit $511B.

And here are the homicide statistics[275] for the years 1994 to 2012 in South Africa:

Year	Homicides per 100,000
1994	66.9
1995	67.9
1996	62.8
1997	59.5
1998	59.8
1999	52.5
2000	49.8
2001	47.8

274 http://en.wikipedia.org/wiki/Economy_of_South_Africa

275 http://en.wikipedia.org/wiki/Crime_in_South_Africa

2002	47.4
2003	42.7
2004	40.3
2005	39.6
2006	40.5
2007	38.6
2008	37.3
2009	34.1
2010	31.9
2011	30.9
2012	31.1

Before 1994, crime figures were not made public. Apartheid land distribution — the creation of large white-owned farms — has left a legacy of violence against white farmers. Unemployment and massive immigration from other African countries has provoked waves of urban violence and rape. And yet, despite this, the real figures fall every year[276], today down to less than half the rate during Apartheid.

It took four decades for the white elites to realize their mistake, and open the economy to all people no matter the color of their skin. The whites lost their privileges yet they also shed their fears and their isolation. And despite the difficulties of building a working society from such a low base, the new multicultural South Africa has done well for itself.

What Ended Apartheid?

Four decades seems infinity, looking forwards, yet that is what we are in for, in my opinion. We might as well take a deep breath and develop real strategies for a positive outcome. Let's start with the question of why Apartheid fell at all. This is a is vital question, because it provides us with our own strategy for a successful outcome. Padraig

276 http://www.saps.gov.za/statistics/reports/crimestats/2013/crime_stats.htm

O'Malley writes on nelsonmandela.org[277], in his article, "Exploring Reasons For The Collapse Of Apartheid,"

> *To get to the understanding that both parties could only accommodate their differences through negotiations and that they could not resolve them through a protracted and indefinitely drawn-out war of violence and counter violence took the better part of a decade.*
>
> *Forsaking war rooms for negotiating tables was not an option particularly palatable to either side, but one dictated by the logic of inevitability. Perhaps a chess analogy is most appropriate. Neither side could achieve checkmate; permanent stalemate was the alternative to declaring a draw. Draws means deals.*
>
> *In short, once both sides came to realize that the one could not hold on to power through its repressive security policies and the other recognized that it could not seize power through an armed "liberation" struggle the options for both became more narrow, and more importantly, more crystallized.*

Here is the key. Even if you cannot win a fight — and it is absurd to think the Spider would lose any fight it starts — you can force the other side to a negotiated solution if you can make it too costly for them to govern. By the mid-1980's, the townships had become ungovernable as people stopped cooperating with the system. The youth stopped going to school, and focused instead on civil protest. You give us no future, they said, so we will not invest in yours.

O'Malley argues that Apartheid was its own cure, in that by breaking South African society apart by color, Apartheid also made it ungovernable. This may be partly true, and it is a good appeal to the intrinsic morality of a sane society, though I'd counter this with the ex-

277 http://www.nelsonmandela.org/omalley/index.php/site/q/03lv02424/04lv03370/05lv03390.htm

ample of the US. That shows a massively segregated country, which exhibits all the signs of collective stupidity, yet is a society robustly under control (please, US, prove me wrong).

Rather, I believe two other factors that turned Apartheid from an obviously profitable strategy to a hopelessly costly one. One was the fall in the cost of communications. Pretoria, isolated and distant, could maintain its regime as long as resistance was disorganized and local. However, it became so easy to report on events, and to carry images of oppression around the world. By the late 1980's the global anti-apartheid movement used electronic bulletin boards and email to organize.

The ability to spread information rapidly and cheaply led to more and more hostility against the regime from around the world. It led to increased support for the ANC. European public opinion was particularly important. It led to massive coalitions between trade unions, political movements, student movements, and more social-minded governments that hurt Pretoria. The economic embargo against South Africa was considered by many to be critical, though I believe it in fact prolonged the situation, by damaging the economic middle class that was essential to political change. I've already written that such actions should be focussed against a political leadership, personally, rather than a country, collectively.

The second factor was, I believe, the cost of weaponry. The fall of the Soviet Union caused Africa to flood with cheap guns like the AK47, and cheap ammunition. The security of the Apartheid regime depended on stability in its neighbors to the north. However, cheap weapons caused first Angola and Mozambique, and then Rhodesia to fall to revolutionary liberation movements that were fiercely hostile to Pretoria, and helped the ANC in every way they could.

South Africa had annexed the neighboring German colony of South West Africa after the First World War. In 1960, the South West African People's Army (SWAPO) started a long fight for independ-

ence that ended only in 1990, when the country finally ended thirty years of internal war and renamed itself "Namibia".

South West Africa was a key buffer zone from which Pretoria could keep the civil war going in Angola, which was a mess after repeated invasions and interventions by the CIA, western mercenaries, Cubans, Zairians, Zambians, and South Africans. While the Cubans trained the ANC and SWAPO, the South Africans and CIA funded Joseph Savimbi's UNITA to create havoc in western Angola. Pretoria similarly spent vast sums in Mozambique, Botswana, Zimbabwe, Lesotho, and Swaziland, to stop the ANC from building stable bases and networks.

In other words, to keep its homeland secure, South Africa found itself dragged deeper and deeper into multiple civil wars and police actions thousands of miles away. And this became more and more costly, and as in the US civil war, in a war based on slaughter, the economics were unsustainable. Despite the Apartheid regime's mercenary armies, the odds are on the cheaper man, as Kipling wrote in his poem *Arithmetic on the Frontier*. "Two thousand pounds of education drops to a ten-rupee jezail," the jezail being a simple home-made gun.

The Spider is emerging, like the Kaiju rising out of the sea, and is aiming to tear down our digital cities. Our global digital society is facing a Bad Guy of massive proportions. And what happens on line resonates through all society. The 2013 movie "Pacific Rim" from Guillermo del Toro is wonderfully trashy, yet deliberately or not, it frames perfectly the existential threat that we face as a civilized society trying to build a better future.

So this lets us predict a road map for the coming global conflict between broad society and the Spider. There will be no apologies by those in power, no restoration of democracy, and there will be no revolution in the streets. There will be no significant armed resistance, nor sustained mass protests of the kind that might topple a fragile dictatorship. The Para-state is not fragile, it is extremely solid, and exerts

control as the Apartheid regime did, with massive investment in military power, and full control of the economy.

We will see an escalation of violence against those seen as a threat to power. There will be more, not less, investment in broad ranging power structures to keep control. Apartheid South Africa built a continental buffer zone out of entire countries. The Spider will seek to do the same, by taking controlling stakes in large on-line businesses. Terrorist attacks will increase, as will the military response in our cities. Protesters will not be arrested; they will simply be shot where they stand, under martial law.

Much, even most of the population will go along with the Spider, fully and unquestioningly. Even when they know the Narrative to be a lie, they will not see any way to escape the cult that they have lived in all their lives. The Spider will pit brother against sister, neighbor against neighbor, slicing away at its enemies. First the terrorists, then the activists, then the leftists, then the anti-social elements.

Then, even as the policy of repression seems to be working, it will drive the creation of a world wide coalition of resistance. This coalition will absorb so much violence and damage that you'd think it would collapse. Yet it will not. Like the black South Africans, civil society has nowhere else to go except onwards. And slowly it will raise the stakes so that democracy turns to dictatorship, law enforcement to military action, and the rule of law into a state of emergency.

And the townships will become ungovernable, and the Para-state will start to see its profits shrink, and it will ask itself, "can we win this fight?" and though it will receive an overwhelming "Yes we can" from the arms dealers, the answer from the businessmen will eventually come back, "We are losing too much money!"

And technology will catch up, and surveillance will become a child's game, and so will fighting it. For every hacker bagged and sent to a federal prison, a hundred more disposable young men will take his place. The communications infrastructure of the Spider will be sabotaged and broken at every turn. Leaks will torment the Spider,

for the more it tries to keep its dealings secret, the more incentive it creates for whistle blowers.

And finally, eventually, the Para-state and its Spider will have no choice except to move to a negotiated peace and a transfer of power to something, someone, anyone who can repair society and bring back the profits. An extraction economy cannot survive without a happy consumer economy to buy its goods.

A Strategy for Resistance

Revolution cannot happen in the streets. When powerful men gather around a table to discuss their enemies, they always keep one eye on each other. There are parts of the Para-state that profit from stability, and there are far darker parts that benefit from chaos. It would be like trying to fight an attacking tiger by beating it with a raw steak.

Revolution must instead happen in our minds. We must break free of the Narrative and experience that Satori shock of the Awakening. It is nothing mystical, just painfully hard work, yet it is essential. Then, we must reevaluate our own lives and how society emerges from our view of the world. The Para-state is no alien occupying force. It is the shadow cast by our own greed and consumerism. Finally, we must write a new Narrative, one based on humanism, a love for all people, no matter their colors, or origins, or crimes.

With a new Narrative, we can resist occupation and make it so unbearably expensive, that we eventually come to a negotiated settlement with the Para-state, and a transfer of power.

How actually to build resistance against an all-powerful occupation? I'm not sure, this would be my first experience of fighting a global criminal conspiracy with nothing more than my keyboard. Here's my best guess:

- Identify, document, and boycott the businesses and business partners of the Para-state. Boycott the products of extraction economies. Develop a low carbon lifestyle.

- Build a new decentralized Internet that is unbearable expensive to spy on — see my proposal in the Appendix.
- Promote the Awakening and obviously, make sure everyone you know has read this book. It's free to download and share, though you can also buy it in paper.
- Praise the whistle blower and the investigative reporter, for she or he is a true hero. Read the alternative media, staying critical of propaganda, and share with your friends and family.
- Document the Spider's predations, from drones to mall massacres, and mourn them loudly. We are one world, and crimes against any of us are crimes against us.
- Accept no official explanations, ever, without evidence and independent verification. Full cynicism is justified when facing compulsive liars. Assume every single notable incident is either allowed to happen or made to happen.
- Accept that we will have to take whatever the Spider throws at us, as we have nowhere else to go. Accept that we will face a long struggle.
- Focus European public opinion on the Spider, especially to isolated and embarrass the UK, which the US depends on as a proxy and experimental playground. Remind European politicians that the US and UK sent armed terrorists into their towns and cities for 40 years.
- Build public opinion in Brazil and India, two nations who potentially hold the balance of power in coming decades.
- Learn non-English languages and teach them to your children. English, my language, has become the language of the occupier.
- Take none of this personally, seek no revenge, no justice, no accounting. That will never happen. What we must strive for is truth, knowledge, global disarmament, and the restoration of democracy.

- Teach the Para-state and eventually the Spider that violence is not the solution, that it is not profitable, and it is not sustainable.

It sounds hopelessly idealistic yet this is more or less what happened in South Africa. It is a vast challenge, like an incoming tidal wave, which I trust the generations to come will appreciate we understood, and were prepared to face.

There is no 1% and 99%. There is only 100%. We are one planet, one species, and we live or die together.

Postface

Thank you for downloading or buying this book. I hope it was as fun to read, and as disturbing, as it was to write. As Richard Feynman said, "Our imagination is stretched to the utmost, not, as in fiction, to imagine things which are not really there, but just to comprehend those things which are there." Please do move beyond reading, to action. Here are some things you can do today:

- Discuss "Culture & Empire: Digital Revolution" on your blog, on Amazon.com, or on hintjens.com. Write a review of the book: that is the best way to encourage others to read it.
- Download the PDF — it's free — from cultureandempire.com, and share it with your friends and family. Of course I'm happy when people buy the paperback or e-book. We all have bills to pay. However, it's more important that we share knowledge than charge for it.
- Join the edgenet project at theedg.es. In our first 3-week funding campaign on Indiegogo we asked for $1,000 and raised $4,000. Money and effort makes things happen.
- I covered a lot of ground. Take parts of my story and expand on them, in your thesis, your own writing, your film making, your software. Remix the words and ideas from this book, because they are not mine, they are ours.
- Sloganize it! I packed the book with quotable one-liners. Find them, repeat them, in presentations, on t-shirts, on your blog. Knowledge spreads fastest when it travels light. See, that was another one. I can keep doing this all day.

And again, thank you. You, the reader, are most important to me.

Pieter Hintjens, Brussels, 25 November, 2013

Appendix: edgenet

The spy state cannot be voted out of office. It eats laws for breakfast and excretes excuses for breaking them. We will either build a spy-proof Internet, that cannot be banned or controlled, or we accept to become slaves.

Let me recap the three main points of attack on the privacy of our communications:

- The centralized servers where we meet to share information. These can be hacked, or their owners ordered to hand over information. No matter what encryption you use between your PC and the server, data is held unprotected on servers.
- The client PCs and devices where we run our browsers. These are often laden with spyware, or hacked individually when the case needs it, in a "targeted attack."
- The broadband connections across which the clients talk to the servers. Broadband providers record metadata and provide it to the authorities as a matter of course.

A full-spectrum attack, such as the FBI's takedown of Freedom Hosting in 2013, hits each of these three vulnerabilities. They arrested the server operator, and with his help, put code on the sites he hosted. This code attacked the users' web browsers, and exposed their IP addresses, and thus real identities, though the broadband providers. Finally they took down the server, killing all websites that ran on it. So much for the Deep Web.

If the Web is not safe, and the Deep Web is not safe, what is? There is only one long term answer, and that is a new web that lives "off the grid," treating central websites and broadband connections with the full distrust they deserve.

Living on the Edge

To build truly secure communities, we must address all three of these weak points. It's not sufficient to improve our encryption to create a more robust Deep Web. Rather, we need a radical rethink of how we build digital communities in the first place. We need a new kind of Internet, which I'll call **edgenet**, that is resistant to all threats except targeted attacks.

Targeted attacks are costly, so the goal of edgenet is to make it unbearably expensive to spy on us, and extremely cheap to guard against this, in other words to reverse the current balance of power where it's extremely cheap to spy on us, and unbearably expensive to guard against it.

edgenet exists without any centralized infrastructure and is essentially invisible to the spy state unless it makes a great effort. Since we cannot trust ISPs with our metadata, we cannot trust the last mile of the Internet[278]. So no 3G or 4G, no ADSL at home or the office, not even dial up modems, for anything that has to be secure. Similarly, since any centralized service is a single point of failure, we cannot trust a web based on centralized services.

Instead of centralized services that we access over commercial broadband, edgenet builds on two alternative technologies, which though not new, have been difficult to exploit until recently:

- True peer-to-peer connections that cannot easily be monitored.
- Distributed services that cannot easily be monitored or broken.

edgenet is not an original idea. People have been trying to build decentralized "mesh networks" for a long time. In the past, building a mesh network was technically hard, since it depended on specialized WiFi hardware and firmware. Some did build these, on a small scale, and there is even an official WiFi protocol for mesh[279] since in 2011. However, off-the-shelf WiFi equipment does not support mesh

278 https://en.wikipedia.org/wiki/Last_mile

279 http://en.wikipedia.org/wiki/IEEE_802.11s

without modification, so the technology is out of reach for ordinary people.

However the vision of large-scale mesh networks running on off-the-shelf hardware and software is becoming more realistic, thanks to the same technology that brought the Internet to Africa, namely smartphones. Smartphones have rewritten the old rules about what is possible on the edge of the Internet. They potentially take the Internet back to its roots, before the web. This sounds retrograde, yet to build edgenet we have to undo the whole concept of a heavily-centralized Web and reconstruct our communications around a very different animal.

We need a "fabric," that is, a decentralized network of computers that can talk to each other without that vulnerable dependence on broadband connections. I'm going to explain how to create a fabric that can stretch at least across cities, and possibly across the globe. Then, we need applications that can use that fabric to create new social networks. One step at a time; this is a delicate story. Let's start with the fabric.

The Invisible Fabric

Once upon a time, the Internet was a worldwide network of servers, mostly in universities, and all more or less equal. If you wanted to run an application like email, or gopher, or FTP, you would log onto a server and work there, in a "terminal window." There were some powerful workstations — like the SPARCstation from Sun — that could speak TCP/IP, though these were effectively servers too, and ran like them.

Then Windows 95, the first decent version of Windows, helped launch the "some are more equal than others" web that dominates today. The combination of a workable TCP stack (originally, Trumpet Winsock, and belatedly, Microsoft's own stack), an affordable home computer, and the graphical web browser formed the basis for cheap and scalable connectivity.

Many people tried to use their PCs as "home servers." One of my popular *fin du siecle* free software programs, Xitami, turned a Windows PC into a fast little web server. Nonetheless, most of us learned to use our PCs as thin clients, especially by 2005 or so, when web applications became powerful enough to replace desktop applications. Today, PCs are rarely used for anything intensive except high-end gaming.

There were some very successful mesh-like applications up until 2005 or so, including Skype (before Microsoft changed Skype to use centralized servers). However even pre-Microsoft Skype and infamous P2P file sharing protocols like BitTorrent all worked through the broadband connection, allowing the ISPs to see all the traffic, filter it, log it, and so on.

The Internet was based on a promise of a smart edge (computers) connected over a dumb fabric (TCP/IP), and then the Web turned that inside out, giving us a dumb edge (thin clients) talking to a smart center (websites). The web model is cheap, scalable, and profitable. However, as we see, it is so very vulnerably to malfeasance. I'm not just speaking of the spy state and its voyeuristic hate of our privacy. Among the crooks, I also count the cartels of broadband providers, the movie and record associations with their lawsuits against people sharing music and movies, and governments legislating what we can say, and do, with whom.

Cost gravity comes to the rescue. Smartphones can do many things, such as break when you drop them, and run up extraordinary roaming data bills. They do three things that interest me specifically:

- They are mobile, so where there are people, there are smartphones, charged and working.
- They are powerful, so where there are people, there are powerful computers.
- They almost all have WiFi capabilities. So where there are people, there are powerful computers, capable of talking to each other.

And of course, for many of us, the smartphone is also our main user interface, for photos, tweets, Facebook messages, email. That means the smartphone in our pocket can act much like those Sun SPARCstations from the 1990's: server and client at the same time. Actually even a cheap smartphone is around 25 times more powerful than those so-called "pizza boxes." Finally, there are enough people carrying smartphones to create viable city-wide meshes. All this is recent, and it's what makes edgenet possible today whereas it was impractical even as late as 2010.

Now I'll explain the details, trying not to get too technical. Most of us know that our phones can connect to the WiFi hotspots around us. It's how we play YouTube videos at home without exhausting our mobile Internet quotas. What few people realize is that two phones can often see each other, and chat, over these hotspots. In other words, without using any broadband, and without any traffic going out over the public Internet.

This is called a "client-to-client" connection. Client-to-client connections work on most WiFi access points (that is, the little box with antennas that creates the hotspot) that you buy, and most that you'll find in cities. There are exceptions. For example the AT&T hotspots in Starbucks across the US do not allow client-to-client connections.

If you think this through, you may see the possibilities. When you are at home, or in the office, or in a café with a friendly WiFi hotspot, you can connect a bunch of phones, tablets, and laptops together in interesting ways. This is not a hypothesis. There are applications that stream video from a phone or tablet to a WiFi-enabled TV, or a TV with some dongle, like Google's Chromecast, attached. In 2011-2012, my firm designed such technology for a large electronics firm, and it's in use on their smartphones today. I also wrote an open source library called Zyre[280] that does this — if you run it on a phone, it will look for any other phone also running Zyre, connect to it, and then let applications exchange data.

280 http://zyre.com

When you are out and about in the street, things become more fun. It's harder to find friendly WiFi hotspots. And even if you do, you have to stay within 10-30 yards of the hotspot for things to work. The "inverse power law" means that if two antennae (like the WiFi access point and your phone) move twice as far apart, they need to use four times as much energy to talk to each other.

All modern smartphones — since 2010 or so — can create their own WiFi hotspots at will, unless the ability has been disabled by the phone company. AT&T, for example. So if you have a smartphone in your pocket that is running Zyre, and you're walking in the street, it would be possible to switch on your WiFi hotspot, and search for other friendly WiFi hotspots, and make opportunistic connections to any other Zyre smartphone. (Don't bother looking for Zyre on the marketplace, it's raw material for programmers to make mobile applications.)

If you imagine a group of friends hiking in the mountains, their smartphones could connect to create a small "cell," to use the terminology of mobile phone networks. However, when the same people are in the city, in a bar, or in a demonstration, at a concert, or even at home, they will be in range of several cells.

The cells aren't fixed like mobile phone cells. Instead they switch on and off and move about randomly, since each cell is centered on one smartphone acting for a while as a WiFi hotspot. Now, a smartphone can be in one cell at a time, and as it moves from cell to cell, it can carry information with it. This creates an "asynchronous mesh," in other words, it's possible for data to move across an entire city, slower than we're used to with broadband, yet still fast enough to be useful.

Let me give an example. A woman takes photos of the police arresting a protester. As she takes these photos, they are pushed out to other smartphones in that cell. Those smartphones move away from the scene, and the photos flow over several more hops, and eventually have reached several thousand smartphones across the whole downtown area. It is impossible to know the origin of the photos, im-

possible to censor them except by physically seizing all phones in the area. That's hard, as they don't have to be visible in order to join a cell.

As people move around the city, the fabric stretches wider and wider. In order to cover the globe, however, I'd exploit those fast-but-stupid broadband connections we all have at home, and create temporary virtual pipes between random pairs, each end of the pipe in a different city. So my PC would connect to a peer in Toronto, then in San Diego, then in Kuala Lumpur, and so on. Modern PCs, fat up from too much gaming, can handle hundreds of such pipes at once. We'd secure and encrypt the pipes using throw-away asymmetric keys. Everything sent on the pipe would be stripped of metadata.

That gives us a global fabric, which I'll dub the "Cellnet." The Cellnet is slow, asynchronous, opportunistic, and works at a human scale, closely tied to our physical movements and proximity to other people. It is a different animal from the Internet we use today, where distance is abstracted to nothing and you never really know who you are talking to. I like the idea of de-abstracting technology.

All of this is possible today, in software, and could take advantage of improvements in hardware and firmware, such as real mesh networking and better batteries. We could build cheap dedicated devices that run the Cellnet: a pocket-sized box that is all battery, with powerful radios, and a couple of blinking lights just because. No screen, no fancy UI software, just a pocket-sized Cellnet node. It could double as a battery recharger for smartphones, which gives plausible deniability to anyone arrested with one, when they are banned. *Kickstarter, anyone?*

The Cellnet would be extremely hard to spy on or disrupt. It is possible to capture WiFi traffic by being physically very close. However it's also quite easy to secure traffic between two peers to the extent that it *cannot* be read or modified or faked. The only way to get information is then to seize the phone itself. While physical seizures (including the old "beat them until they talk" technique) are always an option, they do not scale to billions of people. The spy state can still

tap into traffic that goes across the Internet, by acting as Cellnet nodes. However it can get very little useful from it, and crucially, cannot tie activity back to individual actors.

The Cellnet isn't fully resistant. One can attack WiFi hotspots by sending out jamming signals. However this will disrupt more than just smartphones, and it means having equipment in the right place at the right time. That is difficult and costly, and security is always about raising the costs to attackers.

Which leaves us with the second part of edgenet, namely applications that can work across the Cellnet. I'm going to describe two types of application, two patterns for communication. First, anonymous broadcasting, where one person sends material to anyone who's listening, without revealing their identity. Second, secure messaging, where one person can send a secret message to another person, without an attacker reading the message, modifying it, or sending a fraudulent message.

Anonymous Communities

There is one interesting response to the loss of privacy. Instead of fighting it, that is to embrace it and turn it into an asset. OK, there are people with the power to track us as individuals and map out our lives, so they can manipulate us, or control us. However if we can become truly anonymous, that power has no effect on us.

Most on-line communities depend on identities, in the form of user profiles. It's especially valid for social networks, which boast our photos, biographies, and other tidbits meant to make us look attractive. Flattery to our egos is the sugar kick that keeps us coming back. Perhaps I'm projecting here, yet I certainly use social networks more to see who's retweeted or upvoted my latest amazing comment, than to learn interesting new things. Shame on me.

Strong identities can be healthy for a community. People will say fewer stupid things if it harms their reputation. However "stupid" is quite relative, and strong identities make the speaker more important

than the message. This amplifies some voices while suppressing others. This can make communities less smart than they would be without any identity at all. One alternative is the anonymous community, epitomized by 4chan. This collection of "image boards" is famous for the amount of garbage posted. and it is also the birthplace of Anonymous, one of the most effective on-line communities to ever exist.

I think that anonymous communities are becoming a template for political organization. Digital politics look nothing at all like industrial-age politics. There are no parties, no politicians, no budgets, and no States. Instead, there are armies of self-organized, anonymous, paranoid, and highly competent people organized around insane missions. They are willing and capable of challenging any authority, and they respond to any threat with full-on, unfettered action. It might look like a bunch of out-of-control teenagers, yet it's something much, much stranger.

If you have not read Iain M Banks' work, you might want to. He died in 2013, too young, from cancer. His Culture series[281], which inspired the title of this project, describes some strange worlds. However his most bizarre creations are his machine intelligences, the Minds[282].

The Minds roam the universe doing playful, arbitrary things, until there is a threat to their precious Culture. Then they swing around, and with unflinching psychopathic brutality, no matter how long it takes or how much it costs, they take care of business. Then they get back, metaphorically speaking, to exchanging photos of cats. This is how I see anonymous communities today, and in the future: they are our Minds.

Anonymous broadcasting is very well suited to the Cellnet, it is almost the natural pattern. In fact, it's a pattern that was widely used before the Web, and is even still used in corners of the Internet. I'm

281 http://en.wikipedia.org/wiki/Culture_series

282 https://en.wikipedia.org/wiki/Mind_(The_Culture)

talking about the global discussion system called Usenet[283]. Usenet looks like a combination of email and forums. You subscribe to some topics, and then receive posts on those topic, asynchronously, as your local server chats with other servers. Usenet is where FAQs and spam originated.

Anonymous broadcasting — using the Usenet protocols or something very much like them — also solves the problem of how to avoid flooding the Cellnet.

Social Networks

There are ways to communicate that are considered secure. People do still trust Tor, "Off-the-record" (OTR) chatting, and cryptographic layers like GnuPG[284]. However, as I've explained, these are still vulnerable in various ways. Even if you do wrap your messages in unbreakable end-to-end security, so no server in the middle can ever see the unencrypted data, you are still providing that metadata, which can be sufficient to build a case against you. Simply talking to a person of interest, no matter what you say, can make you a person of interest in turn. Moreover, it's likely that the very use of Tor or other detectable strong encryption from a given network address raises a red flag.

Privacy, the reason for secure messaging, is not a whimsical notion. It is the basis for any relationship that does not explicitly belong in the public domain. It's true that we've gotten used to exposing our relations, like tattoos, on social networking sites. Look how many followers I have! However it strikes me as essentially trashy when two people can become "friends" with a click. Social networks have become a game to their users, and it's a game played with lives.

I think our current "social networks" are little more than emotional candy bars. They look like food, yet are empty of real nourishment. They are addictive, providing an excess of a naturally rare thing,

283 https://en.wikipedia.org/wiki/Usenet

284 http://www.gnupg.org/

namely social company. And I think they make us unhealthy, vulnerable, unfulfilled and, ultimately, not very happy.

A sustainable social network would be a collection of real relationships, not clicks. It would be based on private relationships, since to expose one's relationships makes it them public assets. That may work in some contexts, and certainly in open communities, yet open communities seem to be a different animal than social networks. Each person's social network, that map of our relationships and how important each one is to us, would be owned by each of us, and no one else.

To build up a relationship with a given person, I'd want to call, chat, send photos, share web links, code, and so on, with that person. I'd do this over time, and keep doing it, or the relationship would become stale and uninteresting. This is how it works in real life, and this is how I'd expect my computerized life to work.

I've implied two things here, which I'll say explicitly. One, we don't need a central website to make these exchanges happen. That would be like going to the reception to check if you got post. It is somewhat ridiculous. New messages should arrive seamlessly on our phones or laptops, as indeed they do for the systems that work well: emails, Twitter updates, text messages.

The asynchronous "you got mail" world is much smoother than the synchronous "go to reception to check your inbox" world. In an asynchronous world we have different kinds of stuff going on. Urgent messages that we want to see soon. Normal stuff that can take a few minutes, even longer to arrive. Slow stuff that can take hours or even days to get to us. Again, this is how the real world works, and though I appreciate instant gratification as much as anyone, there is a certain art in building large systems that work just as we expect.

The second thing is, why should the business that operates that social network website own our data? Some people claim the CIA invested heavily into Facebook through its In-Q-Tel venture capital[285]

285 https://www.iqt.org/

vehicle. True or not, Facebook, and firms like it, are able to track our private lives. Even if you do not use this site, every time your friends tag you in a photo or mention your name, that is added to your shadow file.

What's wrong with this picture? Let me give you a one-line definition of "ethics": it is the balance of power in a relationship. When businesses own your social networks, there is no balance of power. That's fine in a world where we can grant unlimited trust to those with power. We do not however live in that world, and I doubt the universe has such a planet in it. Those in power seek power, by definition, and do what they feel they must to retain it.

In a world where the state sees its own citizens as a prime threat to its power, that means building a framework of repression and control. Who you know, where you go, what you say, what you think out loud... these are the data that have sent thousands and millions to their deaths in the past. Agreed, the very notion of the spy state watching and perhaps hunting us, the idea that we live in mortal fear of our own elected governments is highly uncomfortable, close to paranoia.

However, why even take the risk? We can build social networks over the Cellnet. They will be asynchronous and distributed and impossible to trace, except by physical seizure or brute-force hacking of individual devices, the most costly and impractical of surveillance options.

We would want end-to-end security, as GnuPG[286] or ZeroMQ[287] provides, and some form of anonymous routing across nodes, as I've already described. We could exchange security keys by touching our phones together, using the near-field communications, or NFC, feature that many smartphones have. Then we could share data privately, and securely, over multiple hops, whether we're still in the same city, or half-way around the world.

---

286 http://www.gnupg.org/

287 http://zeromq.org

As a user experience, it's simple. I have stuff (code, photos, ideas, documents, music) that I want to share with one or more people. I choose the stuff, click Share (it should be a physical button on the phone) and it pops up my most important groups and people. I choose who to share it with, and that's it.

The actual sharing might take hours or days, as I meet people and our phones exchange data. My stuff hops leisurely across the Cellnet, sometimes getting lost and trying again, until it finds its destination. I don't really care. With enough people connected, data can travel very rapidly and if I really have gigabytes to send, I'll wait until I see the person and we can work over a direct WiFi link.

That's it. It is a short description of what I'd like to help build, or see happen.

Index

Acronyms

Countries

Laws

Organizations

People