Papers

- Crypto Anarchy and Virtual Communities
- State and Terrorist Conspiracies & Conspiracy as Governance

Crypto Anarchy and Virtual Communities

Extended Abstract

The combination of strong, unbreakable public key cryptography and virtual network communities in cyberspace will produce interesting and profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to make the economic arrangements they wish to make consensually.

Strong cryptography, exemplified by RSA (a public key algorithm) and PGP (Pretty Good Privacy), provides encryption that essentially cannot be broken with all the computing power in the universe. This ensures security and privacy. Public key cryptography is rightly considered to be a revolution.

Digital mixes, or anonymous remailers, use crypto to create untraceable e-mail, which has many uses. (Numerous anonymous remailers, in several countries, are now operating. Message traffic is growing exponentially.)

Digital pseudonyms, the creation of persistent network personas that cannot be forged by others and yet which are unlinkable to the "true names" of their owners, are finding major uses in ensuring free speech, in allowing controversial opinions to be aired, and in providing for economic transactions that cannot be blocked by local governments. The technology being deployed by the Cypherpunks and others, means their identities, nationalities, and even which continents they are on are untraceable -- unless they choose to reveal this information. This alters the conventional "relationship topology" of the world, allowing diverse interactions without external governmental regulation, taxation, or interference.

Digital cash, untraceable and anonymous (like real cash), is also coming, though various technical and practical hurdles remain. "Swiss banks in cyberspace" will make economic transactions much more liquid and much less subject to local rules and regulations. Tax avoidance is likely to be a major attraction for many. An example of local interest to Monte Carlo might be the work underway to develop anonymous, untraceable systems for "cyberspace casinos." While not as attractive to many as elegant casinos, the popularity of "numbers games" and bookies in general suggests a opportunity to pursue.

Data havens and information markets are already springing up, using the methods described to make information retrievable anonymously and untraceably.

Governments see their powers eroded by these technologies, and are taking various well-known steps to try to limit the use of strong crypto by their subjects. The U.S. has several well-publicized efforts, including the Clipper chip, the Digital Telephony wiretap law, and proposals for "voluntary" escrow of cryptographic keys. Cypherpunks and others expect these efforts to be bypassed. Technology has let the genie out of the bottle. Crypto anarchy is liberating individuals from coercion by their physical neighbors—who cannot know who they are on the Net—and from governments. For libertarians, strong crypto provides the means by which government will be avoided.

The presentation will describe how several of these systems work, briefly, and will outline the likely implications of this combination of crypto anarchy and virtual cyberspace communities.

1. Introduction

This paper describes the combination of two major technologies:

- Strong Crypto: including encryption, digital signatures, digital cash, digital mixes (remailers), and related technologies.
- Cyberspatial Virtual Communities: including networks, anonymous communications, MUDs and MOOs, and "Multiverse"-type virtual realities.

This paper describes the combination of two major technologies:

These areas have generally remained separate, at least in published papers. Certainly the developers of cyberspace systems, such as MUDs, MOOs, and Habitat-like systems, appreciate the importance of cryptography for user authentication, overall security, and certainly for (eventual) digital purchase of services. But for the most part the combination of these two areas has been the province of the science fiction writer, notably writers such as Vernor Vinge, William Gibson, Bruce Sterling, and Orson Scott Card.

The "Cypherpunks" group, a loose, anarchic mailing list and group of hackers, was formed by several of us in 1992 as a group to make concrete some of the abstract ideas often presented at conferences. We've had some successes, and some failures.[1] The Cypherpunks group also appeared at a fortuitous time, as PGP was becoming popular, as Wired magazine appeared (they featured us on the cover of their second issue), and as the publicity (hype?) about the Information Superhighway and the World Wide Web reached a crescendo.

The site ftp.csua.berkeley.edu has a number of essays and files, including crypto files, in the directory pub/cypherpunks. I have also written/ compiled a very large 1.3 MB FAQ on these issues, the Cyphernomicon, available at various sites, including my ftp directory, ftp.netcom.com, in the directory pub/tc/tcmay.

The Cypherpunks group is also a pretty good example of a "virtual community." Scattered around the world, communicating electronically in matters of minutes, and seeming oblivious to local laws,

the Cypherpunks are indeed a community, and a virtual one. Many members use pseudonyms, and use anonymous remailers to communicate with the list. The list itself thus behaves as a "message pool," a place where information of all sort may be anonymous deposited—and anonymous received (since everyone sees the entire list, like a newspaper, the intended recipient is anonymized).

Legal Caveat: Consult your local laws before applying any of the methods described here. In some jurisdictions, it may be illegal to even read papers like this (seriously). In particular, I generally won't be giving ftp site addresses for copies of PGP, remailer access, digital cash systems, etc. These are well-covered in more current forums, e.g., sci.crypt or talk.politics.crypto, and there are some unresolved issues about whether giving the address of such sites constitutes (or "aids and abets") violation of various export and munitions laws (crypto is considered a munition in the U.S. and probably elsewhere....some nations consider a laser printer to be a munitions item!).

2. Modern Cryptography

The past two decades have produced a revolution in cryptography (crypto, for short) the science of the making of ciphers and codes. Beyond just simple ciphers, useful mainly for keeping communications secret, modern crypto includes diverse tools for authentication of messages, for digital timestamping of documents, for hiding messages in other documents (steganography), and even for schemes for digital cash.

Public key cryptography, the creation of Diffie and Hellman, has dramatically altered the role of crypto. Coming at the same time as the wholesale conversion to computer networks and worldwide communications, it has been a key element of security, confidence, and success. The role of crypto will only become more important over the coming decades.

Pretty Good Privacy, PGP, is a popular version of the algorithm developed by Rivest, Shamir, and Adleman, known of course as RSA. The RSA algorithm was given a patent in the U.S., though not in any European countries, and is licensed commercially.[2]

These tools are described in detail in various texts and Conference proceedings, and are not the subject of this paper.[3] The focus here is on the implications of strong crypto for cyberspace, especially on virtual communities.

Mention should be made of the role of David Chaum in defining the key concepts here. In several seminal papers (for example,[4][5]), Chaum introduced the ideas of using public key cryptography methods for anonymous, untraceable electronic mail, for digital money systems in which spender identity is not revealed, and in schemes related to these. (I make no claims of course that Chaum agrees with my conclusions about the political and socioeconomic implications of these results.)

3. Virtual Communities

Notes: cyberspace, Habitat, VR, Vinge, etc. Crypto holds up the "walls" of these cyberspatial realities. Access control, access rights, modification privileges.

Virtual communities are the networks of individuals or groups which are not necessarily closely-connected geographically. The "virtual" is meant to imply a non-physical linking, but should not be taken to mean that these are any less community-like than are conventional physical communities.

Examples include churches, service organizations, clubs, criminal gangs, cartels, fan groups, etc. The Catholic Church and the Boy Scouts are both examples of virtual communities which span the globe, transcend national borders, and create a sense of allegiance, of belonging, and a sense of "community." Likewise, the Mafia is a virtual community (with its enforcement mechanisms, its own extra-legal rules, etc.) Lots of other examples: Masons, Triads, Red Cross, Interpol, Islam, Judaism, Mormons, Sindero Luminoso, the IRA, drug cartels, terrorist groups, Aryan Nation, Greenpeace, the Animal Liberation Front, and so on. There are undoubtedly many more such virtual communities than there are nation-states, and the ties that bind them are for the most part much stronger than are the chauvinist nationalism emotions. Any group in which the common interests of the group, be it a shared ideology or a particular interest, are enough to create a cohesive community.

Corporations are another prime example of a virtual community, having scattered sites, private communication channels (generally inaccessible to the outside world, including the authorities), and their own goals and methods. In fact, many "cyberpunk" (not cypherpunk) fiction authors make a mistake, I think, in assuming the future world will be dominated by transnational megacorporate "states." In fact, corporations are just one example—of many—of such virtual communities which will be effectively on a par with nation-states. (Note especially that any laws designed to limit use of crypto cause immediate and profound problems for corporations-countries like France and the Philippines, which have attempted to limit the use of crypto, have mostly been ignored by corporations. Any attempts to outlaw crypto will produce a surge of sudden "incorporations," thus gaining for the new corporate members the aegis of corporate privacy.)

In an academic setting, "invisible colleges" are the communities of researchers.

These virtual communities typically are "opaque" to outsiders. Attempts to gain access to the internals of these communities are rarely successful. Law enforcement and intelligence agencies (such as the NSA in the U.S., Chobetsu in Japan, SDECE in France, and so on, in every country) may infiltrate such groups and use electronic surveillance (ELINT) to monitor these virtual communities. Not surprisingly, these communities are early adopters of encryption technology, ranging from scrambled cellphones to full-blown PGP encryption.[6]

The use of encryption by "evil" groups, such as child pornographers, terrorists, abortionists, abortion protestors, etc., is cited by those who wish to limit civilian access to crypto tools. We call these the "Four Horseman of the Infocalypse," as they are so often cited as the reason why ordinary citizen-units of the nation-state are not to have access to crypto.

This is clearly a dangerous argument to make, for various good reasons. The basic right of free speech is the right to speak in a language one's neighbors or governing leaders may not find comprehensible: encrypted speech. There's not enough space here to go into the many good arguments against a limit on access to privacy, communications tools, and crypto.

The advent of full-featured communications systems for computer-mediated virtual communities will have even more profound implications. MUDs and MOOs (multi-user domains, etc.) and 3D virtual realities are one avenue, and text-centric Net communications are another. (Someday, soon, they'll merge, as described in Vernor Vinge's prophetic 1980 novella, True Names.)

4. Observability and Surveillance

An interesting way to view issues of network visibility is in terms of the "transparency" of nodes and links between nodes. Transparent means visible to outsiders, perhaps those in law enforcement or the intelligence community. Opaque mean not transparent, not visible. A postcard is transparent, a sealed letter is opaque. PGP inventor Phil Zimmermann has likened the requirement for transparency to being ordered to use postcards for all correspondence, with encryption the equivalent of an opaque envelope (envelopes can be opened, of course, and long have been).

Transparent links and nodes are the norm in a police state, such as the U.S.S.R., Iraq, China, and so forth. Communications channels are tapped, and private use of computers is restricted. (This is becoming increasingly hard to do, even for police states; many cite the spread of communications options as a proximate cause of the collapse of communism in recent years.)

There are interesting "chemistries" or "algebras" of transparent vs. opaque links and nodes. What happens if links must be transparent, but nodes are allowed to be opaque? (The answer: the result is as if opaque links and nodes were allowed, i.e., full implications of strong crypto. Hence, any attempt to ban communications crypto while still allowing private CPUs to exist....)

If Alice and Bob are free to communicate, and to choose routing paths, then Alice can use "crypto arbitrage" (a variation on the term, "regulatory arbitrage," the term Eric Hughes uses to capture this idea of moving transactions to other jurisdictions) to communicate with sites—perhaps in other countries—that will perform as she wishes. This can mean remailing, mixing, etc. As an example, Canadian citizens who are told they cannot access information on the Homolka-Teale murder case (a controversial case in which the judge has ordered the media in Canada, and entering Canada, not to discuss the gory details) nevertheless have a vast array of options, including using telnet, gopher, ftp, the Web, etc., to access sites in many other countries--or even in no country in particular.

Most of the consequences described here arise from this chemistry of links and nodes: unless nearly all node and links are forced to be transparent, including links to other nations and the nodes in those nations, then the result is that private communication can still occur. Crypto anarchy results.

5. Crypto Anarchy

"The Net is an anarchy." This truism is the core of crypto anarchy. No central control, no ruler, no leader (except by example, reputation), no "laws." No single nation controls the Net, no administrative body sets policy. The Ayatollah in Iran is as powerless to stop a newsgroup—alt.wanted.moslem.women or alt.wanted.moslem.gay come to mind—he doesn't like as the President of France is as powerless to stop, say, the abuse of French in soc.culture.french. Likewise, the CIA can't stop newsgroups, or sites, or Web pages, which give away their secrets. At least not in terms of the Net itself...what non-Net steps might be taken is left as an exercise for the paranoid and the cautious.

This essential anarchy is much more common than many think. Anarchy—the absence of a ruler telling one what to do—is common in many walks of life: choice of books to read, movies to see, friends to socialize with, etc. Anarchy does not mean complete freedom—one can, after all, only read the books which someone has written and had published—but it does mean freedom from external coercion. Anarchy as a concept, though, has been tainted by other associations.

First, the "anarchy" here is not the anarchy of popular conception: lawlessness, disorder, chaos, and "anarchy." Nor is it the bomb-throwing anarchy of the 19th century "black" anarchists, usually associated with Russia and labor movements. Nor is it the "black flag" anarchy of anarcho-syndicalism and writers such as Proudhon. Rather, the anarchy being spoken of here is the anarchy of "absence of government" (literally, "an arch," without a chief or head).

This is the same sense of anarchy used in "anarchocapitalism," the libertarian free market ideology which promotes voluntary, uncoerced economic transactions.[7] I devised the term crypto anarchy as a pun on crypto, meaning "hidden," on the use of "crypto" in combination with political views (as in Gore Vidal's famous charge to William F. Buckley: "You crypto fascist!"), and of course because the technology of crypto makes this form of anarchy possible. The first presentation of this was in a 1988 "Manifesto," whimsically patterned after another famous manifesto.[8] Perhaps a more popularly understandable term, such as "cyber liberty," might have some advantages, but crypto anarchy has its own charm, I think.

And anarchy in this sense does not mean local hierarchies don't exist, nor does it mean that no rulers exist. Groups outside the direct control of local governmental authorities may still have leaders, rulers, club presidents, elected bodies, etc. Many will not, though.

Politically, virtual communities outside the scope of local governmental control may present problems of law enforcement and tax collection. (Some of us like this aspect.) Avoidance of coerced transactions can mean avoidance of taxes, avoidance of laws saying who one can sell to

and who one can't, and so forth. It is likely that many will be unhappy that some are using cryptography to avoid laws designed to control behavior.

National borders are becoming more transparent than ever to data. A flood of bits crosses the borders of most developed countries—phone lines, cables, fibers, satellite up/downlinks, and millions of diskettes, tapes, CDs, etc. Stopping data at the borders is less than hopeless.

Finally, the ability to move data around the world at will, the ability to communicate to remote sites at will, means that a kind of "regulatory arbitrage" can be used to avoid legal roadblocks. For example, remailing into the U.S. from a site in the Netherlands...whose laws apply? (If one thinks that U.S. laws should apply to sites in the Netherlands, does Iraqi law apply in the U.S.? And so on.)

This regulatory arbitrage is also useful for avoiding the welter of laws and regulations which operations in one country may face, including the "deep pockets" lawsuits so many in the U.S. face. Moving operations on the Net outside a litigious jurisdiction is one step to reduce this business liability. Like Swiss banks, but different.

6. True Names and Anonymous Systems

Something needs to be said about the role of anonymity and digital pseudonyms. This is a topic for an essay unto itself, of course.

Are true names really needed? Why are they asked for? Does the nation-state have any valid reason to demand they be used?

People want to know who they are dealing with, for psychological/evolutionary reasons and to better ensure traceability should they need to locate a person to enforce the terms of a transaction. The purely anonymous person is perhaps justifiably viewed with suspicion.

And yet pseudonyms are successful in many cases. And we rarely know whether someone who presents himself by some name is "actually" that person. Authors, artists, performers, etc., often use pseudonyms. What matters is persistence, and nonforgeability. Crypto provides this.

On the Cypherpunks list, well-respected digital pseudonyms have appeared and are thought of no less highly than their "real" colleagues are.

The whole area of digitally-authenticated reputations, and the "reputation capital" that accumulates or is affected by the opinions of others, is an area that combines economics, game theory, psychology, and expectations. A lot more study is needed.

It is unclear if governments will move to a system of demanding "Information Highway Driver's Licenses," figuratively speaking, or how systems like this could ever be enforced. (The chemistry of opaque nodes and links, again.)

7. Examples and Uses

It surprises many people that some of these uses are already being intensively explored. Anonymous remailers are used by tens of thousands of persons-and perhaps abused.[9] And of course encryption, via RSA, PGP, etc., is very common in some communities. (Hackers, Net users, freedom fighters, white separatists, etc....I make no moral judgments here about those using these methods).

Remailers are a good example to look at in more detail. There are two current main flavors of remailers:

1. "Cypherpunk"-style remailers, which process text messages to redirect mail to another sites, using a command syntax that allows arbitrary nesting of remailing (as many sites as one wishes), with PGP encryption at each level of nesting.
2. "Julf"-style remailer(s), based on the original work of Karl Kleinpaste and operated/maintained by Julf Helsingius, in Finland. No encryption, and only one such site at present. (This system has been used extensively for messages posted to the Usenet, and is basically successful. The model is based on operator trustworthiness, and his location in Finland, beyond the reach of court orders and subpoenas from most countries.)

The Cypherpunks remailers currently number about 20, with more being added every month. There is no reason not to expect hundreds of such remailers in a few years.

One experimental "information market" is BlackNet, a system which appeared in 1993 and which allows fully-anonymous, two-way exchanges of information of all sorts. There are reports that U.S. authorities have investigated this because of its presence on networks at Defense Department research labs. Not much they can do about it, of course, and more such entities are expected.

(The implications for espionage are profound, and largely unstoppable. Anyone with a home computer and access to the Net or Web, in various forms, can use these methods to communicate securely, anonymously or pseudonymously, and with little fear of detection. "Digital dead drops" can be used to post information obtained, far more securely than the old physical dead drops...no more messages left in Coke cans at the bases of trees on remote roads.)

Whistleblowing is another growing use of anonymous remailers, with folks fearing retaliation using remailers to publicly post information. (Of course, there's a fine line between whistleblowing, revenge, and espionage.)

Data havens, for the storage and marketing of controversial information is another area of likely future growth. Nearly any kind of information, medical, religious, chemical, etc., is illegal or

proscribed in one or more countries, so those seeking this illegal information will turn to anonymous messaging systems to access—and perhaps purchase, with anonymous digital cash—this information. This might include credit data bases, deadbeat renter files, organ bank markets, etc. (These are all things which have various restrictions on them in the U.S., for example....one cannot compile credit data bases, or lists of deadbeat renters, without meeting various restrictions. A good reason to move them into cyberspace, or at least outside the U.S., and then sell access through remailers.)

Matching buyers and sellers of organs is another such market. A huge demand (life and death), but various laws tightly controlling such markets.

Digital cash efforts. A lot has been written about digital cash.[10] [11] David Chaum's company, DigiCash, has the most interesting technology, and has recently begun market testing. Stefan Brands may or may not have a competing system which gets around some of Chaum's patents. (The attitude crypto anarchists might take about patents is another topic for discussion. Suffice it to say that patents and other intellectual property issues continue to have relevance in the practical world, despite erosion by technological trends.)

Credit card-based systems, such as the First Virtual system, are not exactly digital cash, in the Chaumian sense of blinded notes, but offer some advantages the market may find useful until more advanced systems are available.

I expect to see many more such experiments over the next several years, and some of them will likely be market successes.

8. Commerce and Colonization of Cyberspace

How will these ideas affect the development of cyberspace?

"You can't eat cyberspace" is a criticism often levelled at argument about the role of cyberspace in everyday life. The argument made is that money and resources "accumulated" in some future (or near-future) cyberspatial system will not be able to be "laundered" into the real world. Even such a prescient thinker as Neal Stephenson, in Snow Crash, had his protagonist a vastly wealthy man in "The Multiverse," but a near-pauper in the physical world.

This is implausible for several reasons. First, we routinely see transfers of wealth from the abstract world of stock tips, arcane consulting knowledge, etc., to the real world. "Consulting" is the operative word. Second, a variety of means of laundering money, via phony invoices, uncollected loans, art objects, etc., are well-known to those who launder money...these methods, and more advanced ones to come, are likely to be used by those who wish their cyberspace profits moved

into the real world.

(Doing this anonymously, untraceably, is another complication. There may be methods of doing this--proposals have looked pretty solid, but more work is needed.)

The World Wide Web is growing at an explosive pace. Combined with cryptographically-protected communication and digital cash of some form (and there are several being tried), this should produce the long-awaited colonization of cyberspace.

Most Net and Web users already pay little attention to the putative laws of their local regions or nations, apparently seeing themselves more as members of various virtual communities than as members of locally-governed entities. This trend is accelerating.

Most importantly, information can be bought and sold (anonymously, too) and then used in the real world. There is no reason to expect that this won't be a major reason to move into cyberspace.

9. Implications

I've touched on the implications in several places. Many thoughtful people are worried about some of the possibilities made apparent by strong crypto and anonymous communication systems. Some are proposing restrictions on access to crypto tools. The recent debate in the U.S. over "Clipper" and other key escrow systems shows the strength of emotions on this issue.

Abhorrent markets may arise. For example, anonymous systems and untraceable digital cash have some obvious implications for the arranging of contract killings and such. (The greatest risk in arranging such hits is that physical meetings expose the buyers and sellers of such services to stings. Crypto anarchy lessens, or even eliminates, this risk, thus lowering transaction costs. The risks to the actual triggermen are not lessened, but this is a risk the buyers need not worry about. Think of anonymous escrow services which hold the digital money until the deed is done. Lots of issues here. It is unfortunate that this area is so little-discussed....people seem to have an aversion for exploring the logical consequences in such areas.)

The implications for corporate and national espionage have already been touched upon. Combined with liquid markets in information, this may make secrets much harder to keep. (Imagine a "Digital Jane's," after the military weapons handbooks, anonymously compiled and sold for digital money, beyond the reach of various governments which don't want their secrets told.)

New money-laundering approaches are of course another area to explore.

Something that is inevitable is the increased role of individuals, leading to a new kind of elitism. Those who are comfortable with the tools described here can avoid the restrictions and taxes that others cannot. If local laws can be bypassed technologically, the implications are pretty clear.

The implications for personal liberty are of course profound. No longer can nation-states tell their citizen-units what they can have access to, not if these citizens can access the cyberspace world through anonymous systems.

10. How Likely?

I am making no bold predictions that these changes will sweep the world anytime soon. Most people are ignorant of these methods, and the methods themselves are still under development. A wholesale conversion to "living in cyberspace" is just not in the cards, at least not in the next few decades.

But to an increasingly large group, the Net is reality. It is where friends are made, where business is negotiated, where intellectual stimulation is found. And many of these people are using crypto anarchy tools. Anonymous remailers, message pools, information markets. Consulting via pseudonyms has begun to appear, and should grow. (As usual, the lack of a robust digital cash system is slowing things down.

Can crypto anarchy be stopped? Although the future evolution in unclear, as the future almost always is, it seems unlikely that present trends can be reversed:

- Dramatic increases in bandwidth and local, privately-owned computer power.
- Exponential increase in number of Net users.
- Explosion in "degrees of freedom" in personal choices, tastes, wishes, goals.
- Inability of central governments to control economies, cultural trends, etc.[12]

The Net is integrally tied to economic transactions, and no country can afford to "disconnect" itself from it. (The U.S.S.R. couldn't do it, and they were light-years behind the U.S., European, and Asian countries. And in a few more years, no hope of limiting these tools at all, something the U.S. F.B.I. has acknowledged.[13]

Technological Inevitability: These tools are already in widespread use, and only draconian steps to limit access to computers and communications channels could significantly impact further use. (Scenarios for restrictions on private use of crypto.)

As John Gilmore has noted, "the Net tends to interpret censorship as damage, and routes around it." This applies as well to attempts to legislate behavior on the Net. (The utter impossibility of regulating the worldwide Net, with entry points in more than a hundred nations, with millions of machines, is not yet fully recognized by most national governments. They still speak in terms of "controlling" the Net, when in fact the laws of one nation generally have little use in other countries.)

Digital money in its various forms is probably the weakest link at this point. Most of the other pieces are operational, at least in basic forms, but digital cash is (understandably) harder to deploy. Hobbyist or "toy" experiments have been cumbersome, and the "toy" nature is painfully

obvious. It is not easy to use digital cash systems at this time ("To use Magic Money, first create a client..."), especially as compared to the easily understood alternatives.[14] People are understandably reluctant to entrust actual money to such systems. And it's not yet clear what can be bought with digital cash (a chicken or egg dilemma, likely to be resolved in the next several years).

And digital cash, digital banks, etc., are a likely target for legislative moves to limit the deployment of crypto anarchy and digital economies. Whether through banking regulation or tax laws, it is not likely that digital money will be deployed easily. "Kids, don't try this at home!" Some of the current schemes may also incorporate methods for reporting transactions to the tax authorities, and may include "software key escrow" features which make transactions fully or partly visible to authorities.

11. Conclusions

Strong crypto provides new levels of personal privacy, all the more important in an era of increased surveillance, monitoring, and the temptation to demand proofs of identity and permission slips. Some of the "credentials without identity" work of Chaum and others may lessen this move toward a surveillance society.

The implications are, as I see it, that the power of nation-states will be lessened, tax collection policies will have to be changed, and economic interactions will be based more on personal calculations of value than on societal mandates.

Is this a Good Thing? Mostly yes. Crypto anarchy has some messy aspects, of this there can be little doubt. From relatively unimportant things like price-fixing and insider trading to more serious things like economic espionage, the undermining of corporate knowledge ownership, to extremely dark things like anonymous markets for killings.

But let's not forget that nation-states have, under the guise of protecting us from others, killed more than 100 million people in this century alone. Mao, Stalin, Hitler, and Pol Pot, just to name the most extreme examples. It is hard to imagine any level of digital contract killings ever coming close to nationstate barbarism. (But I agree that this is something we cannot accurately speak about; I don't think we have much of a choice in embracing crypto anarchy or not, so I choose to focus on the bright side.)

It is hard to argue that the risks of anonymous markets and tax evasion are justification for worldwide suppression of communications and encryption tools. People have always killed each other, and governments have not stopped this (arguably, they make the problem much worse, as the wars of this century have shown).

Also, there are various steps that can be taken to lessen the risks of crypto anarchy impinging on personal safety.[15]

Strong crypto provides a technological means of ensuring the practical freedom to read and write what one wishes to. (Albeit perhaps not in one's true name, as the nation-state-democracy will likely still try to control behavior through majority votes on what can be said, not said, read, not read, etc.) And of course if speech is free, so are many classes of economic interaction that are essentially tied to free speech.

A phase change is coming. Virtual communities are in their ascendancy, displacing conventional notions of nationhood. Geographic proximity is no longer as important as it once was.

A lot of work remains. Technical cryptography still hasn't solved all problems, the role of reputations (both positive and negative) needs further study, and the practical issues surrounding many of these areas have barely been explored.

We will be the colonizers of cyberspace.

12. Acknowledgments

My thanks to my colleagues in the Cypherpunks group, all 700 of them, past or present. Well over 100 megabytes of list traffic has passed through he Cypherpunks mailing list, so there have been a lot of stimulating ideas. But especially my appreciation goes to Eric Hughes, Sandy Sandfort, Duncan Frissell, Hal Finney, Perry Metzger, Nick Szabo, John Gilmore, Whit Diffie, Carl Ellison, Bill Stewart, and Harry Bartholomew. Thanks as well to Robin Hanson, Ted Kaehler, Keith Henson, Chip Morningstar, Eric Dean Tribble, Mark Miller, Bob Fleming, Cherie Kushner, Michael Korns, George Gottlieb, Jim Bennett, Dave Ross, Gayle Pergamit, and—especially—the late Phil Salin. Finally, thanks for valuable discussions, sometimes brief, sometimes long, with Vernor Vinge, David Friedman, Rudy Rucker, David Chaum, Kevin Kelly, and Steven Levy.

13. References and Notes

1. The Cypherpunks group was mainly formed by Eric Hughes, Tim May, and John Gilmore. It began both physical meetings, in the Bay Area and elsewhere, and virtual meetings on an unmoderated mailing list. The name was provided by Judith Milhon, as a play on the "cyberpunk" genre and the British spelling of cipher. The mailing list can be subscribed to by sending the single message subscribe cypherpunks in the body of a message to majordomo@toad.com. Expect at least 50 messages a day. About 600 subscribers in many countries are presently on the list. Some are pseudonyms. ↩
2. RSA Data Security Inc., Redwood Shores, California, is the license administrator. Contact them for details. ↩
3. Many crypto texts exist. A good introduction is Bruce Schneier's Applied Cryptography, John Wiley and Sons, 1994. This text includes pointers to many other sources. The "Crypto" Proceedings (Advances in Cryptology, Springer-Verlag, annually) are essential

references. The annual Crypto conference in Santa Barbara, and the Eurocrypt and Auscrypt conferences, are where most crypto results are presented. ↩

4. David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM 24, 2, February 1981, pp. 84-88. Cypherpunks-style remailers are a form of Chaum's "digital mixes," albeit far from ideal. ↩
5. David Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete," Comm. ACM 28, 10, October 1985. This is an early paper on digital cash...be sure to consult more recent papers. ↩
6. The political opposition in Myan Mar—formerly Burma—is using Pretty Good Privacy running on DOS laptops in the jungles for communications amongst the rebels, according to Phil Zimmermann, author of PGP. This life-and-death usage underscores the role of crypto. ↩
7. David Friedman, The Machinery of Freedom, 2nd edition. A leading theoretician of anarcho-capitalism. (Hayek was another.) ↩
8. Tim May, The Crypto Anarchist Manifesto, July 1988, distributed on the Usenet and on various mailing lists. ↩
9. Abuse, according to some views, of remailers is already occurring. A Cypherpunks-type remailer was used to post a proprietary hash function of RSA Data Security, Inc. to the Usenet. (Let me hasten to add that it was not a remailer I operate, or have control over, etc.) ↩
10. article on digital cash, The Economist, 26 November 1994. pp. 21-23.
11. article on digital cash, Steven Levy, Wired. December 1994. ↩
12. See Kevin Kelly's Out of Control, 1994, for a discussion of how central control is failing, and how the modern paradigm is one of market mechanisms, personal choice, and technological empowerment. ↩
13. During the "Digital Telephony Bill" debate, an FBI official said that failure to mandate wiretap capabilities within the next 18 months would make it all moot, as the cost would rise beyond any reasonable budget (currently $500 million for retrofit costs). ↩
14. "Magic Money" was an experimental implementation of Chaum's digital cash system. It was coded by "Pr0duct Cypher," a pseudonymous member of the Cypherpunks list—none of us knows his real identity, as he used remailers to communicate with the list, and digitally signed his posts. Many of us found it too difficult to use, which is more a measure of the deep issues involved in using digital analogs (no pun intended) to real, physical money. ↩
15. Robin Hanson and David Friedman have written extensively about scenarios for dealing with the threats of extortionists, would-be assassins, etc. I am hoping some of their work gets published someday. (Much of the discussion was in 1992-3, on the "Extropians" mailing list.)

Timothy C. May

535 Monterey Drive

Aptos, CA 95003 U.S.A.

tcmay@netcom.com

December, 1994

State and Terrorist Conspiracies & Conspiracy as Governance

Novermber 10, 2006 & December 3, 2006

By Julian Assange

FOREWARD

CRYPTOME

31 July 2010

These essays on conspiracies by Julian Assange (me@iq.org) were retrieved today from his website iq.org. The first from the currently active site, dated Novermber 10, 2006, and the second at archive.org, dated December 3, 2006.

http://iq.org/conspiracies.pdf

http://web.archive.org/web/20070110200827/http://iq.org/conspiracies.pdf

Thanks to Jason Lewis for pointing to this in his Mail On Sunday report.

Julian Assange:

http://web.archive.org/web/20071020051936/http://iq.org/

Sun 31 Dec 2006 : The non linear effects of leaks on unjust systems of governance

You may want to read The Road to Hanoi or Conspiracy as Governance (second essay following); an obscure motivational document, almost useless in light of its decontextualization and perhaps even then. But if you read this latter document while thinking about how different structures of power are differentially affected by leaks (the defection of the inner to the outer) its motivations may become clearer.

The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive "secrecy tax") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption.

Hence in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance.

Only revealed injustice can be answered; for man to do anything intelligent he has to know what's actually going on.

More: http://web.archive.org/web/*/http://iq.org

Part 1

State and Terrorist Conspiracies

me @ iq.org

November 10, 2006

> Behind the ostensible government sits enthroned an invisible government owing no allegiance and acknowledging no responsibility to the people. To destroy this invisible government, to befoul this unholy alliance between corrupt business and corrupt politics is the first task of statesman-ship. (President Theodore Roosevelt)

> While you here do snoring lie, Open-eyed *conspiracy* His time doth take. (The Tempest; Ariel at II, i)

Introduction

To radically shift regime behavior we must think clearly and boldly for if we have learned anything, it is that regimes do not want to be changed. We must think beyond those who have gone before us, and discover technological changes that embolden us with ways to act in which our forebears could not.

Firstly we must understand what aspect of government or neocorporatist behavior we wish to change or remove. Secondly we must develop a way of thinking about this behavior that is strong enough carry us through the mire of politically distorted language, and into a position of clarity. Finally must use these insights to inspire within us and others a course of ennobling, and effective action.

Authoritarian power is maintained by *conspiracy* Conspiracy, Conspire: make secret plans jointly to commit a harmful act; working together to bring about a particular result, typically to someone's detriment. ORIGIN late Middle English : from Old French _conspire_r, from Latin conspirare agree, plot, from con-to-gether with spirare breathe.

> "The best party is but a kind of *conspiracy* against the rest of the nation. (Lord Halifax)

Where details are known as to the inner workings of authoritarian regimes, we see conspiratorial interactions among the political elite not merely for preferment or favor within the regime but as the primary planning methodology be- hind maintaining or strengthening authoritarian power.

Authoritarian regimes give rise to forces which oppose them by pushing against the individual and collective will to freedom, truth and self realization.

Plans which assist authoritarian rule, once discovered, induce resistance. Hence these plans are concealed by successful authoritarian powers. This is enough to define their behavior as conspiratorial.

> "Thus it happens in matters of state; for knowing afar off (which it is only given a prudent man to do) the evils that are brewing, they are easily cured. But when, for want of such knowledge, they are allowed to grow until everyone can

> recognize them, there is no longer any remedy to be found. (The Prince, Niccolo Machiavelli [1469-1527])

Terrorist conspiracies as *connected graphs*

Pre and post 9/11 the Maryland Procurement Office (National Security Agency light cover for academic funding, google for grant code “MDA904”) and others have funded mathematicians to look at terrorist conspiracies as *connected graphs* (no mathematical background is needed to follow this article).

We extend this understanding of terrorist organizations and turn it on the likes of its creators where it becomes a knife to dissect the power conspiracies used to maintain authoritarian government.

We will use *connected graphs* as way to harness the spatial reasoning ability of the brain to think in a new way about political relationships. These graphs are easy to visualize. First take some nails (“conspirators”) and hammer them into a board at random. Then take twine (“communication”) and loop it from nail to nail without breaking. Call the twine connecting two nails a link. Unbroken twine means it is possible to travel from any nail to any other nail via twine and intermediary nails. Mathematicians say the this type of graph is connected.

Information flows from conspirator to conspirator. Not every conspirator trusts or knows every other conspirator even though all are connected. Some are on the fringe of the *conspiracy*, others are central and communicate with many conspirators and others still may know only two conspirators but be a bridge between important sections or groupings of the *conspiracy*.

Separating a *conspiracy*

If all links between conspirators are cut then there is no *conspiracy*. This is usually hard to do, so we ask our first question: What is the minimum number of links that must be cut to separate the *conspiracy* into two groups of equal number? (divide and conquer). The answer depends on the structure of the *conspiracy*. Sometimes there are no alternative paths for conspiratorial information to flow between conspirators, other times there are many. This is a useful and interesting characteristic of a *conspiracy*. For instance, by assassinating one “bridge” conspirator, it may be possible to split the *conspiracy*. But we want to say something about all conspiracies.

Some *conspirators* dance closer than others

Conspirators are discerning, some trust and depend each other, others say little. Important information flows frequently through some links, trivial information through others. So we expand our simple connected graph model to include not only links, but their “importance”. Return to our board-and-nails analogy. Imagine a thick heavy cord between some nails and fine light thread between others. Call the importance, thickness or heaviness of a link its *weight*. Between conspirators that never communicate the *weight* is zero.

The “importance” of communication passing through a link difficult to evaluate apriori, since it its true value depends on the outcome of the *conspiracy*. We simply say that the “importance” of communication

contributes to the *weight* of a link in the most obvious way; the *weight* of a link is proportional to the amount of important communication flowing across it. Questions about conspiracies in general won’t require us to know the *weight* of any link, since that changes from *conspiracy* to *conspiracy*.

Conspiracies are _cognitive device_s. They are able to out think the same group of individuals acting alone

Conspiracies take information about the world in which they operate (the conspiratorial environment), pass it around the conspirators and then act on the result. We can see conspiracies as a type of device that has inputs (information about the environment) and outputs (actions intending to change or maintain the environment).

What does a *conspiracy* compute? It computes the next action of the

conspiracy

Now I we ask the question: how effective is this device? Can we compare it to itself at different times? Is the *conspiracy* growing stronger or weakening? This is a question that asks us to compare two values.

Can we find a value that describes the power of a *conspiracy*?

We could count the number of conspirators, but that would not capture the difference between a *conspiracy* and the individuals which comprise it. How do they differ? Individuals in a *conspiracy* *conspire*. Isolated individuals do not. We can capture that difference by adding up all the important communication (*weights*) between the conspirators, we will call this the *total conspiratorial power*.

Total conspiratorial power

This number is an abstraction. The pattern of connections in a *conspiracy* is unusually unique. But by looking at this value which in independent of the arrangement of conspiratorial connections we can make some generalisations.

If *total conspiratorial power* is zero, there is no *conspiracy*

If *total conspiratorial power* is zero, there is no information flow between the conspirators and hence no *conspiracy*. A substantial increase or decrease in *total conspiratorial power* almost always means what we expect it to mean; an increase or decrease in the ability of the *conspiracy* to think, act and adapt.

Separating weighted *conspiracies*

I now return to our earlier idea about cleaving a *conspiracy* into halves. Then we looked at dividing a *conspiracy* into two groups of equal numbers by cutting the links between conspirators. Now we see that a more interesting idea is to split the *total conspiratorial power* in half. Since any isolated half can be viewed as a *conspiracy* in its own right we can continue splitting indefinitely.

How can we reduce the ability of a *conspiracy* to act?

We can marginalise a *conspiracy*'s ability to act by decreasing *total conspiratorial power* until it is no longer able to understand, and hence respond effectively to, its environment. We can split the *conspiracy*, reduce or eliminating important communication between a few high *weight* links or many low *weight* links.

Traditional attacks on conspiratorial power groupings, such as assassination, have cut high *weight* links by killing, kidnapping, blackmailing or otherwise marginalizing or isolating some of the conspirators they were connected to.

An authoritarian *conspiracy* that can not think efficiently, can not act to preserve itself against the opponents it induces

When we look at a *conspiracy* as an organic whole, we can see a system of interacting organs, a body with arteries and veins whos blood may be thickened and slowed till it falls, unable to sufficiently comprehend and control the forces in its environment.

Part 2

Conspiracy as Governance

me @ iq.org December 3, 2006

> The best party is but a kind of *conspiracy* against the rest of the nation. (Lord Halifax)

> Security gives way to *conspiracy*. (Julius Caesar, act 2, sc. 3. The soothsayer's message, but Caesar is too busy to look at it)

Introduction

To radically shift regime behavior we must think clearly and boldly for if we have learned anything, it is that regimes do not want to be changed. We must think beyond those who have gone before us and discover technological changes that embolden us with ways to act in which our forebears could not.

We must understand the key generative structure of bad governance[^1] We must develop a way of thinking about this structure that is strong enough to carry us through the mire of competing political moralities and into a position of clarity. Most importantly, we must use these insights to inspire within us and others a course of ennobling and effective action to replace the structures that lead to bad governance with something better.

[^1]: Everytime we witness an act that we feel to be unjust and do not act we become a party to injustice. Those who are repeatedly passive in the face of injustice soon find their character corroded into servility. Most witnessed acts of injustice are associated with bad governance, since when governance is good, unanswered injustice is rare. By the progressive diminution of a people's character, the impact of reported, but unanswered injustice is far greater than it may initially seem. Modern communications states through their scale, homogeneity and excesses provide their populace with an unprecedented deluge of witnessed, but seemingly unanswerable injustices.

Conspiracy as governance in authoritarian regimes

Where details are known as to the inner workings of authoritarian regimes, we see conspiratorial interactions among the political elite, not merely for prefer-ment or favor within the regime, but as the primary planning methodology behind maintaining or strengthening authoritarian power.

Authoritarian regimes create forces which oppose them by pushing against a people's will to truth, love and self-realization. Plans which assist authoritarian rule, once discovered, induce further resistance. Hence such schemes are concealed by successful authoritarian powers until resistance is futile or outweighed by the efficiencies of naked power. This collaborative secrecy, working to the detriment of a population, is enough to define their behavior as conspiratorial.

> Thus it happens in matters of state; for knowing afar off (which it is only given a prudent man to do) the evils that are brewing, they are easily cured. But when, for want of such knowledge, they are allowed to grow until everyone can recognize them, there is no longer any remedy to be found. (The Prince, Niccolo Machiavelli [1469-1527])

Terrorist *conspiracies* as *connected graphs*

Pre and post 9/11 the Maryland Procurement Office[^2] and others have funded mathematicians to look at terrorist conspiracies as *connected graphs* (no mathematical background is needed to follow this article).

We extend this understanding of terrorist organizations and turn it on the likes of its paymasters; transforming it into a knife to dissect the conspiracies used to maintain authoritarian power structures.

We will use *connected graphs* as a way to apply our spatial reasoning abilities to political relationships. These graphs are very easy to visualize. First take some nails ("conspirators") and hammer them into a board at random. Then take twine ("communication") and loop it from nail to nail without breaking.

Call the twine connecting two nails a link. Unbroken twine means it is possible to travel from any nail to any other nail via twine and intermediary nails.

Mathematicians say that this type of graph is *connected*.

Information flows from conspirator to conspirator. Not every conspirator trusts or knows every other conspirator even though all are connected. Some are on the fringe of the *conspiracy*, others are central and communicate with many conspirators and others still may know only two conspirators but be a bridge between important sections or groupings of the *conspiracy*.

[^2]:National Security Agency light cover for academic funding, google for grant code "MDA904"

Separating a *conspiracy*

If all conspirators are assassinated or all the links between them are destroyed, then a *conspiracy* no longer exists. This is usually requires more resources than we can deploy, so we ask our first question: What is the minimum number of links that must be cut to separate the *conspiracy* into two groups of equal number? (divide and conquer). The answer depends on the structure of the *conspiracy*. Sometimes there are no alternative paths for conspiratorial information to flow between conspirators, other times there are many. This is a useful and interesting characteristic of a *conspiracy*. For instance, by assassinating one “bridge” conspirator, it may be possible to split a *conspiracy*. But we want to say something about all conspiracies.

Some conspirators dance closer than others

Conspirators are often discerning, for some trust and depend each other, while others say little. Important information flows frequently through some links, trivial information through others. So we expand our simple connected graph model to include not only links, but their “importance”.

Return to our board-and-nails analogy. Imagine a thick heavy cord between some nails and fine light thread between others. Call the importance, thickness or heaviness of a link its *weight*. Between conspirators that never communicate the *weight* is zero.

The “importance” of communication passing through a link is difficult to evaluate apriori, since its true value depends on the outcome of the *conspiracy*.

We simply say that the “importance” of communication contributes to the *weight* of a link in the most obvious way; the *weight* of a link is proportional to the amount of important communication flowing across it. Questions about conspiracies in general won’t require us to know the *weight* of any link, since that changes from *conspiracy* to *conspiracy*.

Conspiracies are cognitive devices. They are able to out think the same group of individuals acting

alone

Conspiracies take information about the world in which they operate (the conspiratorial environment), pass through the conspirators and then act on the result. We can see conspiracies as a type of device that has inputs (information about the environment), a computational network (the conspirators and their links to each other) and outputs (actions intending to change or maintain the environment).

Deceiving conspiracies

Since a *conspiracy* is a type of cognitive device that acts on information acquired from its environment, distorting or restricting these inputs means acts based on them are likely to be misplaced. Programmers call this effect *garbage in, garbage out*.

Usually the effect runs the other way; it is *conspiracy* that is the agent of deception and information restriction. In the US, the programmer's aphorism is sometimes called "the Fox News effect".

What does a *conspiracy* compute It computes the next action of the *conspiracy*

Now we ask the question: how effective is this device? Can we compare it to itself at different times? Is the *conspiracy* growing stronger or is it weakening? This question asks us to compare two values over time.

Can we find a value that describes the power of a *conspiracy*?

We could count the number of conspirators, but that would not capture the key difference between a *conspiracy* and the individuals which comprise it. How do they differ? In a *conspiracy*, individuals

conspire, while when isolated they do not. We can show most of this difference by adding up all the important communication (*_weight_s*) between all the conspirators. Call this *total conspiratorial power*.

Total conspiratorial power

This number is an abstraction. The pattern of connections in a *conspiracy* is usually unique. But by looking at a value that is independent of the arrangement of connections between conspirators we can say something about conspiracies in general.

If *total conspiratorial power* is zero, there is no *conspiracy*

If *total conspiratorial power* is zero, then clearly there is no information flow between the conspirators and hence no *conspiracy*. A substantial increase or decrease in *total conspiratorial power* almost always means what we expect it to mean; an increase or decrease in the ability of the *conspiracy* to think, act and adapt.

Separating weighted conspiracies

We now return to our earlier idea about cleaving a *conspiracy* into halves. Then we looked at dividing a *conspiracy* into two groups of equal numbers by cutting the links between conspirators. Now we see that a more interesting idea is to split the *total conspiratorial power* in half. Since any isolated half can be viewed as a *conspiracy* in its own right we can continue separating indefinitely.

Throttling weighted conspiracies

Instead of cutting links between conspirators so as to separate a _weight_ed *conspiracy* we can achieve a similar effect by *throttling* the *conspiracy* — constricting (reducing the *weight* of) those high *weight* links which bridge regions of equal *total conspiratorial power*.

Attacks on conspiratorial cognitive ability

A man in chains knows he should have acted sooner for his ability to influence the actions of the state is near its end. To deal with powerful conspiratorial actions we must think ahead and attack the process that leads to them since the actions themselves can not be dealt with. We can *deceive* or *blind* a *conspiracy* by distorting or restricting the information available to it. We can reduce *total conspiratorial power* via unstructured attacks on links or through *throttling* and *separating*. A *conspiracy* sufficiently engaged in this manner is no longer able to comprehend its environment and plan robust action.

Traditional vs. modern conspiracies

Traditional attacks on conspiratorial power groupings, such as assassination, cut many high *weight* links. The act of assassination — the targeting of visible individuals, is the result of mental inclinations honed for the pre-literate societies in which our species evolved.

Literacy and the communications revolution have empowered conspirators with new means to *conspire*, increasing the speed of accuracy of the their interactions and thereby the maximum size a *conspiracy* may achieve before it breaks down.

Conspirators who have this technology are able to out *conspire* conspirators without it. For the same costs they are able to achieve a higher total conspira torial power. That is why they adopt it.

For example, remembering Lord Halifax’s words, let us consider two closely balanced and broadly conspiratorial power groupings, the US Democratic and Republican parties.

Consider what would happen if one of these parties gave up their mobile phones, fax and email correspondence — let alone the computer systems which manage their subscribes, donors, budgets, polling, call centres and direct mail campaigns?

They would immediately fall into an organizational stupor and lose to the other.

An authoritarian *conspiracy* that cannot think is powerless to preserve itself against the opponents it induces

When we look at an authoritarian *conspiracy* as a whole, we see a system of interacting organs, a beast with arteries and veins whose blood may be thickened and slowed until it falls, stupefied; unable to sufficiently comprehend and control the forces in its environment.

Later we will see how new technology and insights into the psychological motivations of conspirators can give us practical methods for preventing or reducing important communication between authoritarian conspirators, foment strong resistance to authoritarian planning and create powerful incentives for more humane forms of governance.

Glossary

Blind : restricting the information transferred across the links between conspirators

Connected graphs : a visual representation of connectivity as used in graph theory

Conspiracy, Conspire : make secret plans jointly to commit a harmful act; working together to bring about a particular result, typically to someone's detriment. ORIGIN late Middle English : from Old French _*conspire*_*r*, from Latin *conspirare* agree, plot, from *con*-together with *spirare* breathe. (OED)

Deceive : distorting the information transferred across links between conspirators

Device : something that processes communication by accepting an input from the external environment and/or producing an output that is intended to maintain or change the external environment.

Cognitive device : Where collaborative _device_s yield a *conspiracy* of greater complexity than the sum of the work produced by each individual *device*.

Separating : division of a *conspiracy* by severing the links between conspirators

Total conspiratorial power : Sum of the *weights* between conspirators

Throttling : A means of reducing the *weight* or *weights* between conspirators

Weight: measure of the importance between links (singular)

Weights: *weight* (plural)