



**DECISION SUPPORT SYSTEMS, inc.**

**DSSI**

*METATEMPO: SURVIVING GLOBALIZATION*

---

# DEFENSE IN-DEPTH

---

## DESIGN NOTES

---

MICHAEL WILSON

**DECISION SUPPORT SYSTEMS, INC.**

INFO@METATEMPO.COM

[HTTP://WWW.METATEMPO.COM](http://www.metatempo.com)

---

COPYRIGHT 1997-2001. ALL RIGHTS RESERVED

---

## INTRODUCTION

---

This is a very different sort of paper than what I've normally released for public consumption, and I hope that you, the reader, will bear with me. I have no argument to present, and in fact, there will be very little narrative that flows in a linear fashion. My feeling is that the subject matter is best presented informally and as a number of bullet points (including the liberal usage of bolding to highlight relevant design points), since there is no real order to them, and in fact, many of the points will seem contradictory (you'll understand why when you read them).

As an infrastructural warfare (IWAR) professional of some experience, I have been both the **attacker** and **defender**; this is as it should be, for **both are essential knowledge as complimentary elements**. The role of the defender, however, is not one that I enjoy, or take lightly. Defensive systems, as far as I'm concerned, are elemental, not to be retro-fitted or added on to systems. The implications of such a belief are significant--I don't think people or organizations should hire consultants. Let me qualify that: if you or your organization are bootstrapping your defensive efforts, attempting to manage a crisis, or need to acquire critical skills or knowledge under a well defined but short-term basis, then by all means hire the best that your money can buy. If you are building something that needs security or safety as an essential element, or you need to have a defensive effort in place, **DO NOT 'outsource'**--take the time to acquire or educate staff in-house, augment your ability and knowledge about defensive methodologies, and make certain you integrate the defense into your organization/product/service as an essential element, not a special or temporary one.

And so to the purpose of this paper. You, the wise soul who can and will take my advice, need a starting place, a beginning education; I thought that the best help I could provide you (other than the fact that I'm out there in the net for people who want to contact me) would be to give you some of the basic tools I use to think about defensive systems, then walk you through an example utilization. At times the educational effort might seem didactic, at others to rely on the Socratic method, but I hope it accomplishes its purpose--to make you independent of outside aid except in dire need.

---

## RATIONALE AND DEFINITIONS

---

What I know about defense comes from experience, research, and long contemplation in my chosen field, waging IWAR. IWAR takes its strength from the opponent; as a structure becomes more complex, there is little choice except to specialize and create dependencies and infrastructures; modern social structures are intricate and convoluted networks of relationships, dynamic yet fragile. For this sort of conflict, a solution is not a 'point defense' or 'perimeter defense'--**any hardened point or points can be worked around or obviated**. I truly began to have an appreciation of this while reviewing and triangulating (use of multiple sources to correct for bias) on the history of T. E. Lawrence in World War I, who relied upon the fact that while his **opponent could reinforce any specific point to withstand attack, he couldn't reinforce every point**; IWAR, then as now, relies on this point--there are very few organizations or entities that are **self-reliant**. What is needed in defense is to address this as a fundamental difference in the design, implementation, and operation of elements depended upon in society; **as no one particular point can be made totally independent and secure, then every point will need to be reinforced as robustly as possible**.

Defense-In-Depth (DID) is an **approach to design, implementation, and operation where each and every component, system, subsystem, process, procedure, etc. is looked at to see what threat(s) could occur at that level, and then addressing the threat(s) at that level**. If all threats are handled at level most appropriate, and DID is integrated in from the conceptual stage and not just added-on, then there is an **aggregate effect** of defensive measures throughout entire structure, benefitting from a blend of **active and passive measures**. **Overlapping layers** of protection should integrate in **'forcing factors'**--a

system element or process that **requires confrontation with the security/protection prior to utilization** of that element, and this requires the use of authentication, cryptography, judgment, etc. While not perfect, it supplies a **rigor of thought** that provides an improvement over the prevailing approach, that of neglect of safety and security concerns, or coping with them as an afterthought. DID also requires a dedicated adherence to **engineering rigor** in all design: **extensive testing, redundancy, graceful degradation with 'safe failure,' and essentially hardening of 'targets' in general**. Notice that the collateral benefits are also considerable, leading to higher safety and improved quality.

---

## PROBLEM ISOMORPHS

---

One of the first things you'll note is that when I'm thinking about defense, I'm not drawing distinctions between the material, real world, and the electronic, virtual reality; just as in karate, where I learned that a circular block was the best counter to a straight strike (and vice versa), I've found that low-tech attacks on high-tech targets are commonly the best method (and vice versa again). While the 'terrain' might be different, **neither an attacker nor defender should concentrate, but instead have one foot in each world**.

Just like in communication, where it really boils down to two people telling each other stories, and that everything is always like something else, I've found that I rarely get anywhere by grinding away and thinking directly through a strategy or tactic, but instead by looking at a number of elements that might have similarities--**working through the models to think about the modeled**. What follows are a number of problem isomorphs, **analogies** to help you solve your own problems (this is by no means a 'complete' list--there isn't one; the world is full of lessons) by **thinking about attacks and defenses in various contexts**.

### THE ALPHABET

With a relatively small number of **symbols**, the alphabet is a handy tool--by combining the various symbols we create words, and by assembling even a small number of words in the right order, we convey meaning. Compare this to the burden of pictographic languages and you'll see what an advantage **combinatorials** can be (try to type on a pictograph keyboard some time, then consider the NP-completeness problem).

### ALLOYS

Combine two or more weaker elements together in such a way that your end product is **more than just an additive improvement** and you have an alloy, like bronze, or the conceptual underpinning of DID. This was also called '**synergy**' by R. Buckminster Fuller--the total is greater than the sum of the parts--and is the basis for a rather interesting system of thought.

### NATURAL LAW

When thinking about biological models, remember some key laws of nature:

- ~~///~~ The unnatural act is one that can't be done; **if it can be done, it's natural**.
- ~~///~~ **Mother Nature doesn't care**.
- ~~///~~ **You don't get to vote** on natural laws.
- ~~///~~

### PREDATORS AND PREY

Everything has a **role** in the environment, and more importantly, everything is 'lunch' to something else; because of this, the **behavior** and **attributes** of predators and prey animals can provide worthwhile

models. They've been honed, by the time we're seeing them, for millions of years, a very long **design-implement-test-reiterate** cycle.

## DIVERSITY

Nature is about all the possible combinations (the variations that are derived from four simple chemicals in the genetic code); **nature doesn't play favorites**, but seems to count on **numbers** and **variation**. If you can survive in nature, it is because you have 'run the gauntlet' against **multiple, not singular threats**.

## ADAPTATION/EVOLUTION

Living in a natural environment is a **continual struggle** against that **environment**, the other life in that environment, as well as **chance**. Punctuated equilibrium, in particular, is one of the models used by evolutionary biology; simply put, punctuated equilibrium asserts that a species will remain relatively stable with normal sorts of variation, until an environmental **pressure selects some subset of the population as having greater fitness** for survival ('**adaptation**' by virtue of the being the survivor and having the opportunity to breed because the variation was favorable in the new environment). Such pressures could be of the environment, such as a climate change, or some variation of the **Law of the Minimum**, where the community size and growth are 'controlled' by the factor in least availability, such as food, water, sunlight. An environmental change such as an ice age, drought, or occluded atmosphere would force a **die-back** in a population unprepared to cope with the shift (dinosaurs, inefficient predators, plants requiring regular sunlight). The other pressure would be that of a predator--an increase in their **number, efficiency, or acquiring some advantage** (such as our genetic ancestors did with the creation and utilization of tools), also puts evolutionary pressures on the life inside the environment.

## FITNESS

Fitness is achieved by **surviving in a competitive environment** (a meta-fitness, where the fact that a species exists at all is an indication that it has fitness, even if non-obvious); there are also situations where there is a **continual challenge** for who is the most fit, for example, in the ever-present testing for Alpha position in pack hierarchies, like wolves.

## INNATE VS. ACQUIRED

Some species are born/hatched with innate abilities: spiders know how to make webs, bees know how to build hives and behave in their hierarchy. Other species are born and require a way to **acquire necessary knowledge for survival**. As animals progress up the food chain, the pronounced tendency is toward acquired knowledge, thus it must provide a **competitive advantage**. In humans, acquired knowledge has translated into a **dynamic**, rather than a static, process of knowledge, and has facilitated **progress** (each new generation is able to start in roughly the place where previous one left off). As both innate- and acquired-behavior species are still both widespread in the global eco-system, neither trait alone gives a decisive advantage (in fact, there are trade-offs with each trait; eggs (most 'innate' oriented life hatches) are fragile and require great numbers for a few to successfully reach adulthood, the '**quantity**' approach; mammals, with live birth and acquired traits, have longer gestation periods, require a 'social' structure, and take an significant energy expenditure to successfully bring to adulthood, the '**quality**' approach).

## MEMORY

It follows that any animal that acquires knowledge or behavior has to learn it from another animal that remembers it; **communication and sharing of acquired knowledge** is probably the singular 'tool'

that put civilization where it is. As such, societies have memory as well, a '**community memory**' that provides the total knowledge of the community, and may be 'stored' in individuals, proxies, or static representations. Memory may manifest itself in such obvious ways, but it also appears to occur in primitive life, and does provide some evolutionary advantage--more than just things like tapeworms, but bacteria appear to have complex mechanisms for memory and communication (discussed in their own bullet point further below), as does the immune system (also discussed further below).

## AWARENESS

Sensation, an **awareness of the surrounding and extended surroundings**, begins in simple life forms (**tropism**) and becomes complex, specialized systems in advanced life. With sight for example, predators have eyes placed forward (for **stereoscopic parallax**), while prey have wider fields of vision with eyes farther apart toward the sides of the head. Other members of the animal kingdom have less sensitive vision and more sensitive taste, smell, or hearing--sharks, cats, dogs; the specialized sensory organs appear to be able to **cascade** even a few parts-per-million into a trace that can be **investigated and tested/confronted** to see if it is prey or threat. Awareness translates into what we think of as a **Boyd cycle (orient, observe, decide, act)**, which in some animals is extremely low (sloth), and extremely high in others (again, the top of the local food chain, the best predators). Awareness and action creates a sort of sliding scale, from static to dynamic, that is instructive--the **tighter the loop, the better the control of the situation**. In trauma medicine, for instance, the point of the many technological monitoring devices is to provide ready access to continual dynamic information--a changing situation can be immediately addressed, but only if you know about it. This also applies to investment cycles, alterations of patterns, or things like policies and procedures--**unless there is an awareness, situations usually seem static, which is why they become outdated**. An example of this is spending for defensive systems--budgets get decreased in the absence of an active threat, systems become obsolete which increases vulnerability, this creates opportunity for attack, and after it occurs, budgets go up, spending improves the defense, attacks taper off, and spending goes back down, and so on. **Oscillation** like this is not uncommon.

## REFLEX

Just as an awareness aids the predator in **pursuit**, it aids the prey in **evasion**. Bacteria exhibit simple **fight/flight responses** to stimulus; complex reflexive responses, like an autonomic reflex to pain, are basically **reactive attention** with the intent to **retreat from damage**. On the individual animal level, a reflex action promotes survival by triggering the animal to move away from the threat; this is a reflexive and **not reflective** response, and so **some predators utilize the unthinking nature of the action** to their own benefit (cutting an animal out of a herd).

## MOBILITY

In the world of possibilities known as genetic traits, the **trade-off between armor and speed** plays out. Armored animals, such as the turtle and armadillo, have a lot of natural protection afforded to them by their armor; in fact, predators on this sort of prey **require specialization to penetrate** the armor, and this **specialization makes the predator dependent on the prey species** (linked in the eco-system, where overpredation of the prey species will lead to famine of the predator) and the **limitations of those constraints**. Other animals selected out for **extremes** of mobility--flight or great speed, but this has also left them vulnerable in other ways (thin bones, skewed muscle/mass ratios). Some predators, such as wolves and the great cats, show a nicely rounded 'design'--good mobility, enough mass for the armor of bulk, a shaggy coat.

## FLEXIBILITY

Inherent flexibility, such as a willow against the wind or a reed in the water, conveys an innate advantage as a **response to some circumstance**; acquired behavior and memory provides the greatest degree of flexibility in a larger sense, however. Humans are aided further still by additional **flexibility**--a variable posture, to **cope with a variety of situations**, as well as hands with an opposable thumb. **Open cognitive systems with flexible communication mechanisms and tools** would be impossible without all this--the brain's learning capacity and the flexibility of our communication **interfaces** (mouth, facial expression, body language, hands).

#### UBIQUITY, TEMPO, REPLACEABILITY

The scavengers of the foodchain, what we think of as pests, have the advantage of being robust, but with a **tempo and turnover** in the reproductive cycle that provides an ever increasing population regardless of circumstance; they may yet inherit the earth, be they rat, cockroach, worker ant, or bamboo, who have no need for **individual advantage**, as they are **replaceable and interchangeable**.

#### REPRISAL

While some animals will react to danger with flight, some will **automatically strike**, like some snakes. Other animals rely upon the **acquired knowledge and memory of predators**--poisonous toads, porcupines, or bees are not necessarily lethal, but will certainly make a lasting impression. Wasps, on the other hand, are **respected for their ferocious response even when not provoked**, and so are given a wide berth. Reprisals of these various sort are effective in one respect--they reduce the possibility of the species falling to overpredation, even if **individual members might die to establish the 'validity' of the species' reprisal** (note also the **distinct identification** marks generally on such animals). **Actions have consequences.**

#### CAMOUFLAGE, MIMICRY

Advantage for some is to **look like something dangerous**, something that predators will assume is the real thing, a risk--reptiles that look like deadly snakes, insects that resemble bees or wasps; other animals want to **blend in and not be noticed**--coloring and texture that makes them difficult to be aware of, like leaf insects, or polar bears. Some predators will intentionally look like something harmless or use lures--spiders and their webs. It's hard to generalize, as the mechanism is used by predator and prey, to hide or stand out.

#### OVERSPECIALIZATION

**Specialization along certain lines creates great vulnerabilities.** Dinosaurs were unable to cope when, presumably, the environment had shifted slightly in temperature range; the 'survivors' of those species are those that could migrate to a climate similar to their normal habitat, and they still have to migrate (birds). Specialization upon a type of prey leads to dependence upon the prey population--what affects them, affects the predator. Specialization also occurs to extremes, such as deep sea life living at great pressures, or around volcanos, living with incredible heat and dining upon the noxious by-products. While the dinosaurs couldn't live outside their tolerance range, life at the extremes is probably the origins of all life--mutation and adaptation allowed, over great periods of time and through **incremental change**, the ability for such life to survive in 'normal' environments (evolution is the story of **consequence**).

#### TERRITORY, PERIMETER

Some animals, with ranges or territory, **patrol** and will **consider any competing predator in that territory to be threatening** (and are either **challenged**, as in wolves, or **fought**, as in the great cats); some life, such as cacti and porcupines, established a **perimeter to hold off a threat at a closer but defensible distance**; other animals are as close as the **boundary** of their skin (or fur, which can also act as a sensor

'tripwire'), which has previously mentioned response mechanisms once the **threshold** is crossed (and curiously, once you get past the barrier, the metaphor of territory returns with the immune system, see further below).

## OPTIONS

Burrowing animals, such as gophers or mice, will spend a great deal of time making certain they have **options**--if one tunnel or hole becomes blocked or is the direction of attack, there are many other well-concealed ways to escape. Humans have the greatest ability to **cope with threats** because we've created an enormous number of options, commonly available to any serious individual.

## DIFFICULTY

Some prey are easier to acquire than others; short of a specific specialization, this means that the **more costly or difficult to acquire prey have an advantage over more easily acquired prey--it isn't a matter of being better than the predator, just the other prey**. Animals that live in high places (such as arboreals), or other predators, will **require an extra effort and risk to acquire**.

## CROWD BEHAVIOR

While there can be safety in numbers--herds, packs, and other social structures--**group behavior** can be deadly (lemmings), illusory (predators cutting an individual out of a herd), or backfire (sick, old, or injured being turned out of a pack social structure, denied food, or attacked by former pack-mates). Crowds can be **safe for a species, not individuals**.

## INTELLIGENCE

**Cognitive intelligence** is certainly a factor in being a successful predator (notable **exception**, the shark), but so is 'intelligence' in the 'communication regarding the enemy' sense. As efficient as humans can be at the game of **acquiring knowledge** about things (curiosity is a genetic advantage to species with acquired behavior and knowledge), microbiologic organisms have the advantage--they can directly share beneficial genetic material, allowing them communicate functional intelligence used to respond to threats (which is why there is such a rapid increase in multiple drug resistant bacteria--they collect and amass the new capabilities at a faster rate than humans can develop new anti-biotics). The **combination of attribute and tempo** demonstrate another example of the **danger in being unaware**.

## COOPERATION, PARTNERSHIPS

The primitive **symbiotic relationship** between eukaryotic cells (those with genetic material in a distinct membrane-bound nucleus) and mitochondria make life possible on the planet. **Social relationships** (families, tribes, packs) are essential to acquired-knowledge/behavior species. Long term partnerships, such as the human-canine relationship, have also proven to be beneficial in a number of ways. Any such **relationship leaves a risk/opportunity for abuse of trust**, but on the whole, such systems provide advantage in an eco-system.

## AUTHENTICATION

Social relationships are **dependent upon identification and authentication mechanisms**--the smell of the pack, marking territory, mothers identifying their young by scent (pheromonal identifications that likely allow detection along genetic lines). Humans, advanced in most ways, but deficient in certain senses, **augment their abilities** with additional authentication mechanisms (which rely on the triad: **something you are, something you have, something you remember**).

## RESISTANCE

A microbial that gets past the skin boundary and into an individual has to survive in a whole new, hostile environment. The immune system is an **integrated system** of organs, tissues, cells, and cell products--**antibodies that differentiate body from invader** (authentication by **matching against reference traits** such as DNA or the **presence/absence of antigens**, or 'memory' of exposure through **possession of previously sensitized** lymphocytes), neutralizing potentially harmful organisms or substances. Predators and prey on an entirely different **scale**. Immune systems aren't perfect--they can get out of hand and **attack 'friendly' tissue** (arthritis, allergies), or **ignore threats** such as cancer because they have the correct elements of authentication. Microbials can also **take advantage of the immune response**; I think the mechanism of the HIV retrovirus (the cause of AIDS in humans) is like a 'tar baby'--the virus is 'passive' until something attempts to attack/authenticate it, at which point it attacks (which would explain why it ravages helper T-cells, but leaves other 'prey' alone), and after that it's just a matter of statistics (geometric expansion of the predator against a rapidly reducing prey). Viruses also 'compete' at a **meta-level, taking advantage of sociological behavior** (AIDS through its long incubation period and transmission through sexual contact, or 'kuru,' the laughing sickness, which only spreads through cannibalistic consumption of nervous tissue).

## DECAY

Health is merely the slowest rate at which something can die. Once the immune system ceases to hold them in check, a great number of bacteria begin to dine upon the formerly living; everything truly is lunch for something else, **nothing is wasted**. The **impermanence** of things is important, the **old makes way for the new**, and becomes raw material in the process.

## LAW OF THE MINIMUM

Sometimes referred to as the 'yeast-growth' law, in any ecology the size and growth are '**controlled by the factor in least availability**, such as food, water, sunlight. An environmental **change** such as an ice age, drought, or occluded atmosphere would force a **die-back** in a population unprepared to cope with the shift (dinosaurs, inefficient predators, plants requiring regular sunlight). Predators dependent upon specific prey species are affected by any shift in the prey, usually rather dramatically. Particular bounty, a surfeit in the food supply, can cause a consequential population boom. **Dependencies impose limits or constraints**, and **excess can throw a system out of balance** (growth will expand to the maximum of available resources, whereupon it will limit further growth through the process of meeting its own needs, commonly followed by disastrous consequences).

## A BRIEF INTERLUDE

At this point, I'm going to shift away from biological models; they're interesting and useful, but they can provide a restricted view. For example, efficiency in a predator isn't necessarily a good thing; a predator that is 100% effective at taking its prey soon finds itself starving to death. Even on a limited basis, extreme efficiency in a predator has the **unintended consequence** of making the predator extinct (as with some of the oceanic predators of the Mesozoic era, which seemed to have eaten the larger prey to an extent that they themselves starved off in droves, unable to stay above the **threshold of viability**). Machines, on the other hand, can only aspire to such efficiency; for a machine to maintain 100% efficiency, the **context of operation would have to remain equivalently stable**, not possible under the Law of Thermodynamics (an engine in operation quickly increases the heat, coefficient of friction, resistance of field, etc.).

## MODELS VS. ENGINEERING

Models and simulations (which are also problem isomorphs), such as air flight simulators, can be **reflexive simulations**, oriented around providing experiential exposure to the participant, or **reflective**

**simulations**, oriented at cognition and contemplation regarding the subject matter (where continual experiential exposure at the reflective level translates into improved performance at the reflexive level). Simulations and models can have serious flaws and drawbacks; there is a represented world (the real world) and a representing world (the world of the simulation), and design of the represented world and interaction within it is not trivial. Higher order representations tend to alter the relationships represented; models can leave things out that can't be represented, don't seem important, or for which no adequate constraint/limitation can be created. The **representation is not the reality**, which is why you **shouldn't draw conclusions**--the fact that something works or doesn't in a simulation is no assurance of how it will function under real conditions. That's where models run into conflict with engineering rigor--you don't know the results of a situation until you've been through it. For example, there is destructive and non-destructive testing; if you're measuring material strength you can make a rough guess of a new material's strength, but you don't really know until you try it. What's the breaking point? When it breaks, of course. Do the **test a statistically significant number of times** and you begin to have an engineering understanding of it, not a modeler's understanding.

## BUILDINGS

Buildings have a **purpose**--to be accessed and shelter things; as such, you're already a step behind in making a building, any building, secure. People come and go, and without extremes of **controlled-access architecture**, you can't do much to restrain them. **Support systems**, like heating/ventilation/air-conditioning (HVAC) provide fresh air to the building, and comfort, but have also spread biological agents (Legionnaires' disease) and could spread chemical agents easily. **Convenience** is a serious constraint on security and safety; how closely can a truck get to the building, and how much explosive material could be in that truck, or how many of your heavy, awkward belongings (which you might have to carry the '**minimum safe distance**,' an increasing radius)? **Design trade-offs are particularly key as soon as you attempt to apply any security design to real situations**. What's a realistic **threat assessment**? Like the Titanic, who could think it would happen to you? Most buildings only need to worry about supporting their function--ease of access, comfort, protection from the elements, sufficient parking, a nice view--while others need to consider other factors--blast radius, perimeters, fire control, stable and roving patrols, surveillance points of potential observation, high ground of attack, line of sight for laser gun sights or laser microphones, etc. That's the trade-off in the design--how far off can you push the risk?

## BANKS

Financial institutions provide an **economy of scale--expensive protective measures are cheaper to install and operate if you have many people using them**; of course, such an economy of scale means an amassed fortune, making a bank into a target. **As the risk goes up, so does the return**. Defending a bank, or more properly, what's stored in the bank, is accomplished by many things--guards, alarms, a vault, police response, tagged currency. **Counter-measures** to these systems are difficult, but nothing stands still, and the **risk/reward ratio improves as the risk decreases because of technological development**. There are **inherent flaws in each element, and the elements don't act to shore up the weakpoints of other elements**. Vaults, perhaps the most daunting of the elements, can be drilled, finessed (technological lock mechanisms), strong-armed (the low-tech but always viable option of putting a gun to the head (or the heads of his/her family) of whomever does have access), or have a Houdini done to it (Houdini understood that the security of vaults was '**directional**'--while he couldn't necessarily break in, they weren't constructed to prevent being broken out of).

## PRISONS

I haven't personally figured out the real purpose of prisons; are they for **containment, punishment, or rehabilitation**? This confusion also seems to be on the part of those involved in the prison system--the recidivism rate has been going up, and more prisons are being built to house the 'criminals.'

**Convictions make convicts**--strong beliefs in the immorality of an increasing number of actions (including victimless crime) leads to more laws on the books and more people behind bars. Once inside the system, particularly for those with a long-term sentence, there is no need to be civilized--what more can they do to you? The **'retribution price'** for behavior, the consequence for an action, peaks out--why not kill another guard or inmate if you can, since you are already serving 'life'? Why be taken alive if you know you'll spend any years remaining locked in a cell? To house an increasing number of such amateur game theorists (after all, the criminal plays the game of taking a risk, chancing the 'deterrent' payoff of prison), super-maximum security prisons are being built--layer upon layer of barriers, individual cells, minimal guard/inmate contact, etc. From a purely practical standpoint, they aren't going to work, because they don't **alter the fundamental underlying mechanism of difficulty** by addressing the **risk/consequence ratio**. From a security stand-point, the prisons are overspecialized--a computer failure would be catastrophic, and even little things like the **field-of-vision** on the guard towers is **optimized/specialized** to control inward, leaving them dangerously blind to **attack from outside**.

## NUCLEAR POWER PLANTS

Again, a study in design trade-offs, as well as a reflection of the era in which the designs originate from. The nuclear nature of the plants varies with the process, but in the West, such designs are actually fairly safe--it takes a great deal of **coincidence** (which does occur) to force failure in a great many systems which believe that at the first sign of failure, the **default status** of the plant is 'off.' Plants are designed to gracefully degrade, with a 'safe fail.' Security of the plants, however, is not nearly so well designed; the **'threat model'** of the time when most of the plants were designed or constructed oriented around risks of being taken over, to keep protestors out, and contain any problems. Given the **material, static nature of construction**, they are **outdated to cope with threats that have evolved--'no contact'** as opposed to the old **'no retreat'** profiles. Nuclear plant installations can be attacked and neutralized without ever having to **confront** the security systems, there are no **'forcing factors'** that **challenge the updated threats--**explosives, missiles, etc. This is a problem with any **long-term** or **significant-investment** facility--they become **static** and carry into a period where security measures are largely ineffective, or the **invested cost** in the system is too great to afford replacement (sometime the best thing that can happen is a disaster of such proportion that it destroys the installation or demonstrates the obvious requirement to scrap and build anew).

## AIRPORTS

Civilian air travel went through a major transformation after Black September; many of the **policies and procedures** now used to secure airports around the globe were implemented after a spate of hijackings (**'no retreat'** operations, where the opposition force needs to **negotiate** their way out)--checkpoints, passenger control, baggage search/x-ray, commando raids, etc. This led to an evolution in the tactics used into **'no contact'** attacks--missiles and explosives smuggled aboard the plane (for the same reason landmines are so handy in protracted conflicts--good possibility of 'return' for minimal 'risk'); this attack profile is about to be met with a new round of **countermeasures--**thermal neutron analysis (TNA) machines to detect explosives, armored cargo containers, etc. This still does not address the drawback in **'checkpoint'** mechanisms--as a **'permeable' barrier, it doesn't control all interaction through the boundary, nor does it control the area contained by the boundary**. More importantly, it will lead to another evolution in strategy and tactic--from 'no retreat' to 'not contact,' and eventually to a more refined 'no contact,' such as **binary packages** (chemical weapons), incendiaries (such as thermite, which isn't detected by TNA devices), biological weapons, or even just a little **finesse** (such as **overloading** or **misdirecting** detection such as TNA devices or dogs--possibly by spraying a solution that is detected by sensitive measures but otherwise 'invisible' on large numbers of bags (at baggage check, hotels, rental car agencies, any place with an economy of scale), creating a 'boy who cried wolf' problem (which, incidentally, would also work for smuggling cocaine through border checkpoints)).

## MISSILE SILOS

No longer quite such an issue as during the Cold War, silos demonstrated some interesting methodology, as well as a few crucial flaws. As a static installation, they had **no mobility**, and thus became **prime targets in any 'first strike'** scenario; while silos were important, the real issue of the Cold War were the ballistic-missile submarines--run silent, run deep, launch for a **retributive strike**. Another key issue was the **complexity** of the entire missile delivery system--**command and control** with the potential for a need to cope with links and nodes out of order or mobile, **communication** mechanisms like packet switching, security and **cryptography**, background investigations, **reliability/availability/serviceability** (RAS) of all the systems involved, etc. Some very **reliable engineering** came out of the process except for the one thing that really mattered--**nobody could know if the whole system would work until it actually had to work**. Could the missiles be launched? Would they make it over the pole? Worse yet, what if the system functioned, but there was a human **loss of nerve**? The systems weren't automated (not after a few thousand **false alarms** in a year), so **human judgment** was necessary at every step of the process. What if the **redundant systems**, two humans at independent panels needing to turn special keys simultaneously, failed because one of those men refused? Of course they were issued side arms, which became the primary security threat inside the silo, as well as having escalated a launch order to a very personal game of nerves with very high stakes. I think anyone with an awareness of the situation breathes easier knowing that such installations are no longer critical to depend upon.

## AUTOMOBILES

Cars transformed the world (**mass production**, **erosion of distance**, **independence** from muscle power, **social transformations**, etc.), and they provide some basic lessons. Shortly after cars became available, along came the locks and keys--stealing something that was not only portable, but helped steal itself was too sweet for some to pass up. As with any locks, **they don't prevent the problem, they only 'raise the bar'--the skill level of the perpetrator needs to increase as the sophistication of the security device does**. Modern vehicles **integrate security systems** in during the production--it is **cheaper**, they are more **effective** (particularly 'cut out' mechanisms that terminate function, and alarm systems that call for help via radio or cellular phone (audible car alarms that depend on 'local' attention through noise are so sensitive and lacking in **discriminating judgment** that they've created their own 'boy who cried wolf' situation, and became a nuisance)), they help the **value** of the vehicle, etc. Of course, an effective high-tech solution that raises the sophistication bar has also been met with a low-tech solution, the carjacking (**waiting until the valid user of the car deactivates the security system and activates the function, then commandeering it**); now the response appears to be implementation of **reprisals** (while car theft tended to be non-violent crime, carjacking is violent by nature, and so has 'justified' the increase of the risk/consequence stakes). Another issue with cars is safety--mass at high velocity can be dangerous; this has led to very good design and engineering (in particular, the **design methodology** is worth taking a look at), as well as inventions such as the airbag. Of course, the airbag, in actual use, has been a **solution nearly as bad as the problem**, as well as the fact that short supply has made vehicles equipped with the airbag system a specific target for theft of the **component system**. The overall 'social contract' known as the 'rules of the road' is a study in mutual **trust** and **distrust--accidents**, the variable mathematics of **insurance**, and the curious contradictions of certain 'games' (for instance, in accidents involving drunk drivers involved in a collision with another moving vehicle, the injury rate for the drunk driver is far lower than for the other party, who also has an incredibly high fatality rate; drunks may have accidents more frequently, but once in an accident, you're better off being the drunk) help to round out an already bizarre confluence of points to consider.

## TANKS/ARMORED CARS

Another study in design trade-offs: **armor versus mobility**, with the need for storage, the potential for **offensive weapons**, the need to make **coordination of such complex system within human management ability**, and to not make them **so sophisticated that they defy use or repair under real world conditions**. A decisive element in Blitzkrieg, **improper estimation of their potential when designing and implementing** the Maginot Line defense (a '**checkpoint**' system) led to the fall of France in World War II. After that, tanks came to dominate much military thought (particularly for the Soviets and NATO), but **strategically and tactically superior systems** such as the helicopter have had more impact in conflicts after WWII, primarily because of their better **mobility, tempo, and versatility**.

## GUNS

Robert Heinlein commented that **an armed society is a polite society**; his logic was that if the **potential threat of reprisal was unknown but potentially high** (you don't know if the person you are going to mug, rape, rob, or carjack is carrying a concealed pistol), it would inspire an Oriental level of politeness (developed in an era when men carried katana and weren't ashamed to use them if they felt threatened or offended). Studies in regions where the reprisal potential is high--large numbers of **concealed weapons** in the hands of the citizenry, areas with high coverage of 'undercover' police, automated systems which summon immediate help (home or facility alarms, patrolled facilities, automobile systems which radio or phone for help)--tend to bear out the logic; it **raises the bar**, which **convinces the perpetrator to go elsewhere** (incidentally, crime in neighboring regions tends to increase, so it isn't quite a 'good neighbor' policy).

## RADAR/SONAR

The point of radar was in extending the ability to sense and be aware of your surroundings out to the point of the horizon, and it has led to some educational countermeasures. Earliest was **jamming**, the attempt to **flood the reception system ('overload')** with so much information that it was useless. There have been 'ghost' systems, used to **create phantoms** on the reception gear, perception of objects where no objects are--again, the 'boy who cried wolf' of **misdirection** and **confusion**. At a tactical level, chaff serves the same function, dumped for short-term confusion of a missile lock, or to deny the ability to all the players on the field. **Stealth** hopes for the opposite effect--absorb the signal or reflect enough in a direction away from the receptor to not leave a **recognizable signature**. Given the level of sophisticated electronic countermeasures as well as stealth technology, the fact that radar is still used shows another **game theory point--it might be useless under certain conditions, but nobody is willing to give it up just the same**. With sonar, the game is slightly more interesting because of the medium. Active sonar provides you with information, but also provides information on yourself to anyone using passive systems. **Interpretation** of sonar information is much harder than of radar, going beyond engineering skill to manage. Stealth is an entirely different process--making as much of your propulsion and activity as quiet as possible. One of the great questions which only could have been answered by a full NATO/Warsaw Pact conflict was how the Soviets would have coped with the SOSUS system (a geographic array of passive sonar systems used to track Soviet submarines through chokepoints)--**like any checkpoint system, it had flaws**, but would the Soviets have made the attempt (for instance, overloading the SOSUS system by detonating an underwater nuclear device for the potential of destroying the sensor gear, or at least providing enough **cover noise** for wide scale jamming)?

## COUNTERFEITING

Making fraudulent copies of tokens of value or exchange is cutting out the middle man in an economic equation--what is the **cost per unit to make the item in relation to what you can exchange it for, and what is the risk price?** The security measures put into the token are the **direct cost per unit--the manufacturing cost is almost negligible if you can achieve an economy of scale** in production. For currency, the security measures are many--engraving, paper, colour(s), texture, inlays,

watermarks, serial numbers--and technology can readily address all these. The primary issue is **reproducibility**--if the original manufacturer can do it, why not an independent party? Prior to U.S. currency moving to an inlay of a teflon strip in the paper, the easiest method to solve the hardest issues (paper and texture) was to bleach the lowest value currency, and print a higher value on it. Since **currency has no intrinsic value**, this form of counterfeiting will always be possible; while the economics have shifted slightly (it is now more costly per unit because of having to use special paper and processes rather than old bleached currency), the underlying economic issue is unchanged, the **creation of valuable tokens for a favorably small cost**. A currency as a token of value is 'self authenticating'--the countermeasures to counterfeiting are intended to validate the token as having an exchange value, as opposed to being a reference against the bearer. Once the production of the fraudulent version reaches a certain quality, it has the same authentication as the original, and passes for valuable. Cheques and credit cards, on the other hand, also have no intrinsic value, but are a **token and authentication mechanism to verify a financial relationship** (between the bearer and the financial institution), and thus have a greater potential value than currency (incidentally, this is what 'electronic cash' brings to currency--cryptographic verification of a relationship as well as self authentication). Authentication mechanisms--signature, hologram, magnetic strip, photograph, corroborating identification, reference against a remote database on a per-transaction basis, etc.--are all far better than what goes into currency, but as the **potential upside of a fraudulent transaction becomes greater, so does the reward for subverting the system**. Creation of cheques can occur with **proper research** and a computer with a laser printer, an extremely low cost of production (there are **collateral costs**--cut-outs, transaction costs, etc.), but because of bank clearing procedures, each fraudulent transaction is high-risk; credit cards have a greater hurdle for production (although truckloads of card blanks have been stolen at a time, as well as the equipment to emboss), and require research to obtain accounts to **mimic** a financial relationship with, but each **per-transaction risk** is lower because of **automation reliance**, and the perpetrator immediately possesses some value from the transaction. As the **cost of production to potential value of token ratio** improves, the skill required increases, but not usually the costs, and variably the risk--art fraud, for instance, requires skill and talent, but is relatively cheap, potentially high return, and as the discovery is potentially embarrassing to all parties in the transaction, even if discovered it has minimal repercussion.

## PORTFOLIO DIVERSITY

Investing is risky; investment in a single thing means that **success or failure is dependent upon the factors** affecting that one thing. Portfolio **diversity** is the mechanism for **hedging risk**--by investing in a **number of different things that are affected by different factors, the chance of suffering a catastrophic loss is lowered** (based on how well the **diversity balances the factors of dependency linkages**). In a healthy economy, where most things are going well, the best hedge and portfolio diversity is to invest in indexes or across the whole market--some things will surely go down, but most will go up (but note that the '**upside**' of winners is averaged out against the '**downside**' of losers; this is why 'trading' or selective purchase has greater potential and greater risk than the safer 'investing' or portfolio orientation). This is the essence of thinking about design trade-offs--**balancing the dependency factors in the system against the threat and risk potentials that the system might encounter**. Social systems hedge with a great deal of diversity--there are a range of potential disasters or problems on a regular basis, so it is necessary to have fire departments, paramedics, hospitals, police (and here there is further diversity--patrols, police on call, specializations), and so forth. **Concentration on one or only a few things leaves exposure to situational risk, while hedging with diversity leaves you less dependent on circumstance.**

## ALCOHOLICS ANONYMOUS

AA is a support group for people with a problem (starting with the **recognition that they have the problem**); dealing with the problem **isn't a quick solution, but something to be managed** over the course of a lifetime. There **aren't any easy answers**. What AA does provide is a process for **mentoring**,

awareness that you aren't alone, **sharing of information and resources**, and continual **positive reinforcement**. It might be an odd foundation for it, but they have a sense of **community**.

## KNOTS

While maps are about representations of **boundaries**, the topography of knots are ways of looking at things like **friction**; knots don't exist in frictionless worlds, and some knots only hold together when **under pressure**. Friction at interface boundaries, like tension between people or ideas, is natural and probably essential. Some situations have too much **confusion** and friction (see the **Gordian knot**), and can be **obviated with a simple approach**.

## STATES OF MATTER

Water (H<sub>2</sub>O) is interesting in how it **shifts to fit its context**--as a solid, it **retains its form but is brittle**; as a liquid, it **conforms to the shape of its container**; as a gas, it **escapes containment**. The ability to shift to a context is critical to surviving in the new context, like a fish out of water (most of them die, but a few of them didn't, and they're our ancestors).

## ASSASSINATION

There is no person (or small group) so protected, so independent of the world, that they cannot be eliminated. **Dependence on key personnel is always risky** this way; but note that **management, including political, is not necessarily a dependency relationship**. The **loss of a key point will have a cascade effect** throughout a system; the full consequence is almost always impossible to map.

## PIRATES

During a lull in the naval wars between the British and the French, **great numbers of skilled personnel knew only one thing**--fighting on the seas. Given a choice of starving or turning to independent plunder, those chose the latter. During the brief period between the wars, pirates managed to imperil trade, and establish a thriving black market from which a great deal of people (such as the American colonies) benefitted. **Skilled and trained personnel, at loose ends, will do what they know best, and you can't take the training back**; the **unintended consequences** of a score of covert wars and the end of the Cold War are again producing pirates--industrial espionage operatives, terrorists, mercenaries, etc.

## DRUG NETWORKS

The 'drug war' is not a social issue (although viewing it as a consequence of the state of the political economy, with legions of 'refugees in-place' opting out of coping with their lives does have merit) but an economic one. Drug networks supply a product to meet a demand; the fact that (some) drugs are illegal changes the economic system from one of **'opportunity cost'** (the mark-up on a price to compensate the person offering the product for taking the risk that there may be no purchaser) to one of **'risk premium'**--the risk of participating in the economic exchange (arrest, death, loss of product) means that the mark-up is at least 100% at each step. When a transaction is completed successfully, the premium turns into profit, a significant amount. There are other economic exchanges with a risk premium--medicine for example, where the risk of failure or perceived failure can be the death of a patient and criminal/civil liability. Take the risk successfully enough times and you can make a great deal of money; in the case of a physician, the **entry cost** is a great deal of education and training, but in the drug trade, there are no barriers other than the willingness to participate in the risk. The consequences of these facts are what make drug networks so

incredibly **robust**: the **finances** of the participants in the network are astounding, allowing the purchase of equipment, personnel, skilled personnel (attorneys, accountants, security and intelligence, etc.), bribery (paying a million or more U.S. dollars to border control to allow a shipment with 500 times that value through is a wise economic investment), and so forth; and the **replaceability** of any member or 'node' of the network (dealer, distributor, 'soldier,' smuggler, laundry, even leader) is incredible--lose a dealer, you'll find another; lose a shipment, send another; lose your banker, they'll be banging the door down to offer their services; the head of the cartel is arrested or killed, someone else steps in. It would take an attack of **100% efficiency--all nodes, all links, simultaneously--to shut down one of the networks**; miss even the smallest bit, and they'll be grafted onto another network, or grow a new one. Even if such an operation were possible, the territory of the removed network would either be taken over by another, or the **context would spawn a new one**. The 'drug war' is being fought with military hardware and military tactics, but the enemy is something that even the military can only aspire to--a network that can lose links, nodes, product, personnel, anything, and remain functional enough to re-establish. Turn-over or loss has no impact, other than to turn **tempo** to the advantage of the networks--loss of less capable personnel, with steady improvement in the community-at-large. The only solution would be to **change the context**, which would return the risk premium back to an opportunity cost, much as happened in the U.S. after the 18<sup>th</sup> Amendment was repealed and Prohibition ended--whereupon the networks that had profited from illicit alcohol moved into other criminal endeavors where the risk premium was intact.

## LABOR

A key point of Marxist thought, and its greatest underlying mistake, was a belief that labor and material combined to create value, taking into no account the **knowledge** or **skill** behind the labor. This is a case where workers in skilled trades are not interchangeable or automatically replaceable, but well defined work processes, like assembly lines, did seem to confirm the belief of Marxists and Taylorists (Frederick Taylor, known for two concepts--management itself was a skill independent from the process managed, and that work processes could be reduced down to quantifiable, simplistic enough processes that could be optimized and performed by unskilled or minimally skilled workers--both concepts which I believe are fundamentally incorrect in a knowledge-based economy). **Investment does not imply value--**regardless of what resources are spent on something, it can still be ineffective, inefficient, and inutile.

## PERCEPTION

Individuals have varying perceptions (attempt to get two different recollections of the same event and you'll see what I mean; this is correctable through **triangulation**, using many independent points of observation on an event to attempt an evaluation of the objective reality), but on some things, there can be a **collective perception**. A collective perception might be of an objective event, such as the fact that it is raining (but is that a good thing, or a bad thing--some people like rain, others don't, and then there is context to factor in), or have an **impression** that has been **manipulated** (for instance, through **propaganda**). One of the longest standing supports of the Soviet system was the collective impression of the citizenry that the State Security apparatus, the KGB, was all-powerful, all-knowing, that informers were everywhere, and that the slightest variation from orthodoxy would meet with rabid reprisal--so even with a great deal of hate for the system and disbelief, the citizenry either **passively accepted** State action, or **actively collaborated** (after all, someone else would just do it if they didn't, and if you participated with zeal, you might have an opportunity to gain **privilege**--better to be the oppressor than the oppressed). The collective perception of the power of the State fell apart rather dramatically in 1991 with the general uprisings in support of the democratic movement; once the perception of State power was shattered, the Soviet system just evaporated. Mohandas Gandhi demonstrated a similar fallacy to win Indian independence from British rule--**without the consent of the governed, 'law' needs to be backed by force; non-violent non-cooperation** met with armed reprisal, and by **exposing the reprisal actions in**

the world media, the British were put in a spot, talking about being a civilized, beneficent power that in reality did violence to a non-violent subject people. The **shame factor** cannot be underestimated nor overestimated--exposure of Israeli or Chinese oppression has little impact in the world media because of a combination of propaganda, power position, manipulation, playing the 'victim,' and a general disregard for world opinion.

## SCALE

Borders are **too big to control; ideas are too 'big' to destroy**. An appreciation of the scale of things can prevent **'tilting at windmills,' ineffective measures because of unrealistic appraisal**. Scale is rapidly shifting because of technology: in some ways, the **world is a smaller place** because of transportation and communication; in other ways, **power has been scaled down** to the individual, who can leverage him- or herself in significant ways. One plane, carrying one bomb, can level a city; no amount of bombing short of total destruction can destroy an idea.

## NON-LOCALITY

Technology has **eroded the conceptual limitations of distance and time**--the world is a place where people or objects can get/be sent to most any spot in a short period of time, and information 'travels' almost instantly. As **geographic boundaries erode**, people begin to associate with other ways to **differentiate** themselves--racial, ethnic, religious, language, etc. **discrimination** (in a 'set theory' sense). As everything begins to meet non-locally, then **everything becomes local** (just as when 'everyone' owns something, nobody does); **over-the-horizon** weapons like missiles or information warfare become factors to account for, making **threats harder to estimate** through simple processes.

## EXPEDIENCY

**Tempo** of normal society has increased, creating an **expectation of instant gratification**. To provide **immediacy** of service in **realtime**, processes need to be quantified and an attempt made to automate them; the actual function of processes, in particular the judgment involved in processes, is **difficult to quantify**, and **non-trivial to reduce to rules** or even fuzzy processes. **Automated judgment** starts with an attempt to quantify an already biased/flawed process, and then establishes constraints or rigid approximations, further **distorting** the outcome.

## SECRECY, COMPARTMENTALIZATION

Security or safety that relies upon information not being discovered or disseminated is inherently flawed--**information defies attempts to control it**. Compartmentalization is dangerous in an organization if it doesn't work, as well as if it does (a '**double bind**,' where either 'state' of a possible decision/action leads to an error); boundaries to **inhibit the flow of information** require all parties to adhere to observance of them; if boundaries are observed, they create **specialization, removing the possibility of cross-fertilization or correction**, and create a **deliberate narrowing of perspective** (this piece of information relates to that piece of information, and so on--but in this case, the **chain of relationships** is truncated at an **arbitrary** boundary). The result of compartmentalization of information or function and thus specialization, is bureaucracy (**hierarchy comes from control and dependency**, and in this case, control of dissemination of information) and **inertia (areas of specialization remain focused on narrow perspectives** and thus resist or don't have information that allows **dynamic re-assessment**).

## FOOTPRINTS

**Actions have consequences**, and they also leave a **trail--noise, scent, footprints, heat trail, etc.** It is the **observer effect--existence in an environment affects the environment.** Physical **indications decay or degrade** over time, but **digital indications can be timeless; 'rollback' of actions or transactions** can be accomplished through proper **interpretation** of such traces/logs.

## MOMENTUM

**Movement is essential for action**, but movement in a direction has **inertia** (objects in motion tend to stay in motion, unless acted upon); such inertia can be added to, like a running man thrown in the direction he is running, which can **exceed the ability of the object to control** its actions, or leave it moving **faster than can be managed in its OODA (orient-observe-decide-act) cycle.** This is the underlying principle of some martial arts, like judo or aikido, or in tactical military principles (let your opponent rush past your position, then attack from what is now their rear). There is **conceptual momentum** as well, allowing a sort of **ontological judo--guerrilla** or terrorist attacks can be intended to promote a general military or police crack-down, raising the general discomfort level for more people, thus promoting greater dissatisfaction with the governing body (such as the activities of terrorist groups attacking in Israel--the crack-down from the Israelis in reprisal makes all Palestinians suffer, creating growing dissatisfaction with the peace process, Israelis, and the Palestinian Authority).

## TRAILING VS. CHECKPOINTING

**Surveillance** can occur through **active measures** of following the watched party, or through **passive measures**, observing it at **checkpoints.** Both methods have strengths and weaknesses: tailing can provide a complete record of activity, but can betray to the observed that they are being watched; checkpoints might not be noticed, but require a great deal of resources to cover all possible options, or they might be by-passed, and they don't provide an account of what happens outside the observation of the boundary position. Both methods also **assume that the 'threat' is previously defined--neither pursuit nor checkpoints can track the unknown.** During the Cold War, U.S. submarines would attempt to tail Soviet submarines (but could lose them), and Soviet subs were tracked at **chokepoints** by passive sonar devices (which might miss them, or could have been destroyed, overloaded, or subverted) based on their 'signature.'

## DEPENDENCY

A **forced reliance or necessity** means **linked situations or conditions; hierarchy is maintained through dependence**, where the health or success/failure of the dependent party is partially or wholly **reliant on factors outside of their control.** This can also be an acquired state, like addiction or habituation, which leaves the dependent party in a **subordinate and controllable position in the relationship.** Dependency can be **mitigated or removed through establishing and maintaining diversity in relationships**, particularly where needs must be met, but independence from the supplier is essential.

## MONOMANIA

An **obsessive pursuit** of a single object or idea can be destructive (Moby Dick), or be important to **survival** (in a tactical situation, where focus on intent or survival is essential; this may mean that **subordinate desires or concepts**, such as codes of conduct or morality, are temporarily discarded). **Automation by its nature is 'monomaniacal'--thorough and complete, although commonly inflexible.**

## GENERALIZATION

Assigning something into a **category** or **set** can be done by **abstraction**, ignoring specifics that make things unique in order to **conceptualize** them and **compare** them with other known (and usually simpler) things. **Polarization** is common--man/woman, black/white, good/bad, up/down, in/out, yes/no, rich/poor, etc.--and lends a **concreteness** and **specificity** that is rarely found in objective reality. Identification into a set is by **comparison to a reference member of the set**, and leads to the **assumption that items in the set act similarly** (which may be true or not true). As Dumas commented, all generalizations are bad, including this one.

## MAPS

Maps are about the **boundaries** or differences between one thing and another; terrain maps show borders, commonly arbitrary boundaries saying "this is one place, that is another" but such boundaries may indicate **radical shifts in context** (such as one country with a free and open social contract, another with a limited, dictatorial regime). Boundaries are **thresholds, interface points with transmission, interaction, and relationships** that need to be recognized. Maps are also generalizations or models, and as Alfred Korzybski noted, the map is not the territory (**the representation is not the thing represented**).

## TOOLS

Anything that **facilitates a function** is a tool; tools act as a way to **extend performance** of a function (as a hammer allows force to be transferred to a point, or a telescope extends the range of an eye), or **allows leverage** (shifting direction, like a pulley, or screw). Tools derive their usefulness from humans or human interaction, and by themselves are limited; **augmentation** of humans is the essence of a tool.

## CHANNELS, MEDIUM

**Interaction occurs in a conceptual space** that utilizes the tool of a medium for transmission; overt channels are obvious **mechanisms of interaction** (print, speech, etc.), but the parties of the communication recognize that the ability to interpret signals across the channel is a common ability. **Covert channels** are those intended to have **limited recognition**--rare or 'dead' languages (like the use of Navajo in World War II by the U.S.), sign language, morse code, microvoltage fluctuation of computer processors. Covert channel mechanisms may be unnoticed or **look like 'noise' rather than 'signal'** to the unaware party--steganography or other cryptography, or low throughput mechanisms that may not be recognized as communication (for instance, I once used the file protection bits in a UNIX system, flipping one bit on or off at a periodic interval, to transmit data across a 'secure' protected file boundary--patience is a virtue).

## CONSTRAINTS, DESIGN, EVALUATION

Science, oddly enough, has its roots in mysticism--alchemy, which was interested in transmuting base metals into valuable ones. Looking for a shortcut to wealth happened to develop the **scientific method--experimentation (testing and observing) and repeatability (processes performed identically produce the same result)**. Learning about cause and effect--an understanding of **consequence, patterns, and reactions**--led to chemistry, physics, etc. Such is basis of modern **engineering--application of the principles learned through experimentation**. This has also led to a process of **continual improvement**--learning from failure (such as in airplane crashes--find the cause, improve the design, until the next accident, which more is learned from, improving again, and so on). **Constraints** are only understood through testing, by **evaluation under observable variance in condition to achieve outcomes** ('testing to failure'). Evaluation is in the form of a **metric** ('X amount of force or heat causes Y

amount of damage'), but some testing can have **diminishing returns** ('penetration testing,' which can only demonstrate failure, not the positive of functional security).

## JUDGMENT, RESPONSIBILITY, TRUST

**Perceiving and distinguishing relationships accurately** is the basis of judgment; 'good' judgment means having accuracy in **contexts that are similar or of merit**, and is **context dependent** (good 'medical' judgment doesn't translate to good judgment in other areas). In hierarchical relationships, judgment is important to the function, as **authority over a decision or dependency should equate to being responsible/accountable for the outcome of a decision**. **Dependence on judgment and the willingness of someone/something to be held accountable for outcomes resultant from judgment is the basis for trust** in relationships. **Integrity is non-violation of the trust relationship**.

## INITIATIVE

Independence is being **trusted to use one's own judgment, free of constraint or dependency**. In military forces, the main composition of standard forces do not have independence, they are to operate under command inside a rigid hierarchy; special operations forces (SOF) are specifically chosen and empowered to exercise independent initiative to accomplish mission objectives, and may be trusted to select such objectives.

## SERIAL VS. PARALLEL/SIMULTANEITY

Human attention can only be **focused on a limited number** of items at one time; individuals can only be in one place at a time. There are two ways to **degrade human capability--to wear them down over time (fatigue), or to overload their abilities by requiring more capacity than they can bring to bear (either cognitive or by needing to be in more than one place, a physical impossibility)**. **Individual capacity** becomes a critical factor in most situations: fatigue of his troops eventually forced the defeat of Napoleon; emergency services such as fire, police, or medical workers are stretched thin handling heavy demand on a regular basis, and are typically overwhelmed in disaster situations. Massive pressure brought to bear, **'overpressure,'** is the effective mechanism of weapons of mass destruction--extreme heat and shock from atomic/nuclear weapons, mass exposure and overload of neutralization/treatment mechanisms with chemical/biological weapons, and mass outage/subversion with information warfare. The point is to **leave the target unable to cope with the scale/magnitude of the effect**. Attempts to mitigate fatigue or overpressure is the purpose of a **reserve--squirrels store nuts and bears pack on weight for the winter, military forces attempt to leave an uncommitted number or soldiers/materiel available, and corporations try to maintain capital reserves**. A reserve is a **stored resource of general utility set apart for potential use**. In the event of a **cascade, a runaway collapse, or extended adverse situation, even reserves can be insufficient**.

## TOLERANCE, FEEDBACK

**Permissible deviation and operation inside a range** is an ability of life and machine alike--animals are able to survive in certain ranges of temperature, pressure, chemical composition, etc.; machines are built to **function inside a specific contextual range**. Straying outside the tolerance, or **context shifting**, can have adverse affect--like the Challenger disaster when the O-ring deformed due to its being outside of operational ranges of temperature, or the likely theory of extinction of the dinosaur because of the climate change. Life and machine both attempt to maintain a **homeostatic relationship** with the environment--temperature control in the body is regulated and maintained, and **variation outside the tolerance meets with a correcting feedback response** (shivering to generate heat through molecular/muscle action if too cold, breaking a sweat if too hot); machines have similar systems, which tend to **oscillate inside the**

**tolerance** (such as with steering an automobile--you don't keep a dead-straight course, but vary side to side, where the average direction or approximation is the end result; thermostat controls of HVAC).

## VULNERABILITY, RISK, CONSEQUENCE

**Assessment and management of the potential for damage or loss** is crucial; awareness of the range of possible risks can be met with measures to address the risks, weighing off **costs and effectiveness against the repercussions**. **Consequences** are sometimes difficult to predict and manage--**you don't know what you don't know**, so the unexpected can always occur, or **assumptions** can lead to poor conclusions. Poor assumptions can lead to poor function--for example, a straight-jacket might constrain the insane, but a calm, reasoned approach (and some flexibility) can obviate the function. **Assessment** will also lead to trade-offs between **precaution and reaction**: for instance, once germ theory was accepted, measures were taken to inhibit the spread of pathogens from contact; the introduction of anti-biotics, and liberal application of such drugs, led to lax behavior in hygiene (if a patient became infected from lax procedure to prevent contamination, you just treated them with a drug therapy); evolution of multiple drug resistant (MDR) forms of diseases now means that lax procedures spread microbial agents that defy treatment. Modern epidemiology is faced with a number of MDR strains of diseases that could have been drastically slowed through an adherence to precaution/prevention as opposed to lax behavior with reactive measures. Consequence and failure do need to be accounted for and managed--**damage control, controlled failure** ('safe failure' through a **graceful degradation**, or **channeled failure**, like the pressure safety valve on boilers), or the use of **redundancy** (where function or judgment is confirmed through 'tell me twice' or 'tell me three times').

## ANOTHER BRIEF INTERLUDE

This hasn't been an **exhaustive list**--it was an attempt to provide a good **cross section of concepts** to get you thinking on your own about defense. You might disagree with some of them, that's fine, just move on. But the list is a cognitive tool to provide your own **baseline**--as you consider or work on your own defense-in-depth issues, you can quickly scan through the assembled material, and **see what might apply**, or what **ideas might be generated**; I would expect the reader to be able to draw his or her own numerous problem isomorphs for many of the points I've made. The world contains **many risks and outright threats**, and they need to be **addressed with a range of appropriate options for response**.

---

## PROBRIEF DESIGN EXAMPLES

---

The next set of sections are going to attempt to put into practice some of this thinking to show you how I generally start. First I'll walk through the design process, then I'll use the versatility of cryptography three ways: to design a defense-in-depth against computer viruses, to think about an enterprise-wide system for information management, and then in an application, a model money laundering network.

## DESIGN/DEVELOPMENT PROCESS

Creating defensive systems 'on the fly' during a crisis is not my favorite thing to do; as you might expect, **the earlier you can get security and safety thought about in the loop, the better off everyone is**.

An **awareness and acceptance of the need** is crucial--without it, security/safety is an afterthought, and ends up requiring comprehensive redesign, this time with an awareness and acceptance. Whether this is tamper-proof pills, integrating security/safety into an automobile design, protecting a building, or securing a computer, a proper assessment and evaluation at the start of a project will make all the difference. As an experienced opposition force (opfor), this is an easier task for me than perhaps for you,

so let me remind you of **the simple rule of thumb--if it can go wrong, it will**. The best tools are **systems analysis--organizational analysis**, or I'm personally fond of **Yourdon**--and then playing out as many **'what if' scenarios** against the system as I can. For example:

- ☞ Over-the-counter pain medication suppliers should have immediately been worried about tampering; tampering is like other **'no contact'** methods, with a great number of benefits and very few drawbacks to someone being cautious. The **nature of the product itself doesn't change**, but the packaging certainly does--gel-caps, special seals, printed warnings, community education.
- ☞ As much hype as airbags receive, auto design for security and safety has been an 80+ year engineering task--crumple zones, special frames, dedicated subsystems (anti-lock brakes, alarms), restraint systems, rollbars, rules of the road, education. The more **safety and security mechanisms layered into the design and implementation, the easier the task** should be for the end-user (unless they over-rely on the technology, as with any 'armor,' or they selected for style rather than function, a poor design trade-off).
- ☞ Buildings have tended to be made 'safe'--fire, earthquakes, weather--rather than 'secure'--bombs, missiles or other projectiles, chemical/biological weapons, etc. Design trade-offs attempt to make buildings functional for people (windows, HVAC systems, easy access, parking) with measures adequate to safety concerns (reinforced concrete) but inadequate against determined threats. **Hardening targets** is impossible, except in **'spot' circumstance**, which leaves the remaining majority of targets 'soft.'
- ☞ A solid **needs assessment**, coupled with a **laundry list of 'worst case scenarios'** to help as a **metric for design trade-offs**, leads to a **conceptual design**. This is an **iterative process**; as designs get laid out, they must be tested against various metrics. Any conceptual element that is not already a part of standard engineering should be **'rapid prototyped'** to gauge it more accurately than mere supposition. Out of this will come a design that has been subjected to various evaluations and trade-off decisions made (these assumptions should be documented as thoroughly as possible); **independent review at this point is critical**, and my recommendation is to have it **performed by more than one party (at least one other domain expert, and one ruthless bastard, at a minimum)**, to review the assumptions and decisions. **Conceptual errors should be handled with going back to the assessment stage and building back up** (one of the few items in the U.S. Department of Defense design criteria [Rainbow series] that is correct); **design is the most important stage of the entire development process**, for as costly as it might be, once an invested cost in implementation is underway, mistakes become more costly or impossible to correct.

**Implementation** is a management headache all of its own; I personally start with a solid design, and then specify out my **feature/affordance specifications**, timeline, and a resource commitment. If you can assign confident numbers to all three values (**features, resources such as finance and manpower, and timeline**), you are engaged in an engineering project; if you can only assign numbers to two of the three, you are in development (and the third value may oscillate wildly out of control); if only one value can be assigned (your design specification), you are engaged in research; if you haven't even got a solid design, face it, you're experimenting. Management of the four types of implementation efforts are very different, and mistaking one for another is a source of great disaster in many projects.

Upon completion of an implementation, it must be **installed/utilized and pass acceptance testing**; dig back out the assumptions and see how they fare under real world pressures, and if you address the requisite needs. Regardless of success or failure, the **process is iterative**--go back to the beginning and start again: **time has passed, and nothing stands still**. Don't get too distressed--most of it will be **re-usable**.

Somewhere along the way, of course, someone also took the time to **document** the process (a guide to success as well as failure), as well as write the **manuals/documentation** for those who will use the end result. My belief is that **any security/safety system that requires extensive documentation for use is a failure**; on the other hand, I've had to open 'child proof' caps for people who couldn't get the hang of it. Incidentally, I don't consider **policy and procedure** to be an element of documentation, but processes that **require their own design and implementation cycles**, just as any other process; assumptions that they can be developed by fiat explains why many of them don't pass the 'laugh test' in operation.

## AN ANTI-VIRAL SYSTEM FOR COMPUTERS

It may not be politically correct to admit to this, but I wrote my first micro-computer based virus in 1981, and I was already experimenting with concepts derived from **biological models** for a few years, so it wasn't a new experience for me. After a good deal of reading and experimentation, I had learned a great deal about what translated well into digital form--the key was to spread the smallest possible bit of code (assembler at the time), which might be by getting the processor to execute the code (**active measures**), or by letting the user make the copy themselves (**passive measures**). Passive measures were the hardest, and **more sociological than technical**; at the time, computer piracy was an interesting pastime (copy protection was a game, they lock it up, you take it apart; I still remember having a flash of insight, later referred to as 'boot tracing,' that **no matter what access protection they layered, a linear processor still had to step through it to the end, and if the computer could do that, so could I**), and by attaching a virus to a popular piece of pirated software, the greedy bastards would spread it themselves (a fact which I'm certain the software publishers of the day would have taken morbid delight in knowing).

Active measures were complicated, as there was a great deal of **variation**, and so I experimented with a number of mechanisms. Attaching to an application by changing the operating system 'handles' to the file were my first attempts (an OS looks at its reference list and goes to the first block, where a handle points to the next block--this why you might get fragmentation, since you might not have enough contiguous blocks to store files on a disk); it was simple to attach a block as the 'start' point for an application, whereupon it would check a counter to see if it was time to activate. Another variation was a virus that could survive a warm-boot; it could hide in a buffer space used to handle the operating system, and then spread to any uninfected disk that was put into the computer. Eventually I started to play with more extreme variations: 'binary' viruses where one half would spread harmlessly until it met up with another half, or what appeared to be a data file; 'polymorphic' viruses, my attempt to convert something I had written for worms over to microcomputers, a way to cross machine boundaries (it was clunky and never did work right), but that could self-alter to fool checksums (I even had a set of functions that would 'rotate,' different bits of code, thus changing the way something was programmed--drawback, you either carry the 'spare' versions along just in case, or dump them after you reconfigure; it ended up flipping a pseudo-random coin to decide which) and 'signature' analysis (the 'no op' becomes quite handy); while I didn't have the resources to test it, I even wrote an odd bit of viral code that was a small calculator, but that would process messages to resolve logical problems (this was before I encountered Smalltalk), an attempt to use viral propagation to solve a parallel programming problem I was having (incidentally, years later when I got access to a hypercube then a massively parallel system, I found a few flaws, but the design worked).

So I knew more than a bit about the functioning of computer viruses on microcomputers when I noticed that some software companies were making good money with their anti-viral packages. I had tested a number of viruses against the packages and thought them pretty flimsy--they look for a viral signature, which has some serious flaws:

~~to~~ **to be detectable, the signature has to be stable** (you can vary it with polymorphics);

~~when~~ **when you detect it, that means you already have it, and by then you may be too late**, depending on the **function** and **latency** built in. I knew this was dangerous, since I wrote a variation which, first thing off, integrated into the OS and used a public key system to encipher

and decipher the files stored past that time--yank the plug (or it dies on its own), you lose your files. Another 'crypto' variation I wrote would run an approximation of a transcendental number to a certain point in the sequence (say the millionth digit of the natural number), use that as a cipher key, then wipe itself out--the data was retrievable, but only after much recalculation (thus providing computation lead-time, another concept I played with, a way to force a quantifiable 'time delay' before someone could read a message);

~~✍~~ **you don't know what you don't know**--a new virus that hasn't been analyzed yet, and information distributed pack out to software users, is essentially invisible;

~~✍~~ **the software itself is susceptible to Hume's epistemology, it has no way to be certain it itself hasn't been subverted.**

[Note that these are common flaws of any checkpoint system.] To me, these flaws meant that any software solution to the viral problem had to be addressed in hardware, and with certain techniques (how wrong I was--when I tried to go to market with a version of what I outline below, I discovered I made a poor economic trade-off decision; software might not be totally effective, but it was 'mostly' effective, and cheap, while my system required hardware modification (I couldn't get a computer manufacturer interested in integrating it into the motherboard and drive controller for a number of reasons, among them the necessary integration of a DES chip) and was more expensive):

~~✍~~ First, to stop viruses from spreading on their own, all applications needed to be verified before they are allowed to execute. This meant that built into any execution of an application, the system would first the pass control to the hardware sub-system which would perform a cryptographic hash function on the application; I used the DES Message Authentication Code (MAC) because it was reasonably fast and accepted. What do you compare the MAC against? A MAC list stored in the hardware sub-system with logic gates to handle secure access--programmed array logic that would pass control of system I/O to the sub-system, have it MAC an application when first installed, then store it; upon execution, the hardware would go 'autistic' by cutting itself off from the system, 'zero-ize' the buffer, pull the MAC reference out of the internal list, toss the MAC into the buffer, then gate back off the MAC reference list and open access of the sub-system back to the system. MACs of applications would also, in a perfect world, have a 'tell me twice' from the vendor, where the hash would be documented in a public forum (and signed with a cryptographic signature) for additional human verification. If the MAC of the stored application didn't match the reference MAC, the application wouldn't be allowed to execute, and would be zeroed out of the buffer; the application would have to be re-installed and verified before it could be run. Since the operating system would be the first application to run, the boot process would have to be under control of the subsystem, which would MAC the OS on load (handy, because you could also check the file allocation table (FAT) and confirm it). MAC functions will tumble if even a single bit of the original is altered, and so there was a reasonable assurance that the application verified hadn't been altered from the reference hash. Applications could also be ciphered (the default selection); any attack that did happen to find a way to 'add' itself onto such an application would turn to noise (as the application was deciphered, turning it into executable code, the virus would get transformed into noise, and cause a failure interrupt that would be trapped by the system and come to human attention).

~~✍~~ Applications sometime change, or worse yet, data viruses can be a problem, where the application confirms, but execution is passed to an unconfirmed piece of data that wasn't MACed. So all file loads were modeled into a memory map, and the stack was monitored at any flagged/privileged function (when the admin mode of the sub-system was active, meaning the rest of the system was locked out, and direct access to the card was linked to the interface, you could flag any routine used by the operating system as being dangerous or disallowed; dangerous functions required 'tell me twice,' with a hardware confirm prior to execution (like file removal, format of disks, etc.) by

turning a key, and disallowed functions were halted and the attempt logged). Whenever such a function was requested, the memory map was checked to be certain execution never strayed to a point not verified.

- ✍ To prevent viruses from exploiting other processors, or to attempt to run Trojan attacks, memory prior to boot (warm, usually) was zeroed out, as well as all buffers and peripherals.
- ✍ Given the fact that the system essentially had transaction management in place, all transactions were logged; based on system resources (disk capacity was fairly small in the days when this system was built), transactions could be layered so that file overwrites or removal didn't occur except virtually until the system was pulled into administration mode and each was confirmed independently. This allowed a sort of 'deep undo' for the OS, with roll-back being possible, since until the sub-system did it, files weren't actually altered or removed.
- ✍ Lots of minor little features and tweaks, but all of them depending on cryptography or good rational process control (like an experimental part of the system that had all the sub-systems (video controller, drive controller, peripherals) using point-to-point session-to-session, very light cryptography to communicate inside the machine, including for functional requests; any virus, worm, or Trojan that got into the system wouldn't be asking for functions in the right way).
- ✍ Fundamental design principle of the system? Cryptography allows the system an automated judgment factor in deciding what is a valid execution element of the system; by MACing applications and checking against a reference list, the anti-viral system provides a virtual immune system, able to check each application to see if it really has approval to execute on the processor, like an organic body comparing suspect DNA to see if it is part of the body or not. Compare this with the design assumption of anti-viral software--specific analysis of stored applications against known viral signatures, previously encountered pathogens. A perfect world would support both elements--the hardware system provides the original 'immune' response, while a software system can act like a community vaccination program, inoculating the public against known, but not yet personally encountered, threats.

Flaws with the hardware system? DES chips were a munition, and so would have required an export license to use; even if the chip was limited to only authentication functions (MAC only), it would still have needed approval in the U.S., and besides, if I had crypto on-board, I was going to use 3DES, which I did. There was some crypto overhead, maybe a 20% speed loss in access, with the boot taking about three times as long as it would have without the system (it could be cut down to only MACing the OS, then applications upon execution, but in safe mode, it MACed all applications in the FAT table). The pricepoint was higher than software systems--about five times higher, with the tradeoff that you had all the security and safety functions; it was a bit pricey, but if the system were integrated in, that would go way down (anyone out there know an interested computer company?). Installation of the system required a hardware card, with a strap to go into the motherboard socket for memory management, a strap to the drive controller, and a battery for the memory on the card. Management of the system required extra time and care, including the 'tell me twice' confirmation by turning the physical key to confirm certain functions. How did it function in practice? I ran every known sort of virus at the time (300+ from the outside world, and a number of custom ones, based on inside knowledge of the system, written for the occasion), and none of them could spread, or gain access to the microprocessor to execute--100% success, but at a high cost in terms of capital, time, performance speed, utilization of system resources, etc. (the astute reader will note that a virus from a software manufacturer might slip through, coming in under shrink wrap, and getting MACed; it does, however, run into constraints by the system on privileged functions, and if software vendors use cryptographic signatures, there is also accountability and liability). A working defense-in-depth system to prevent infection from computer viruses, with control measures in place as a back-up strategy, but a dismal market failure.

## ENTERPRISE PROTECTION--A CRYPTOGRAPHIC SECURITY MODEL

Was the anti-viral exercise a wasted effort? It didn't pay off in the marketplace, but the methodology that went into it extrapolates to protecting modern and future computer networks. Defense-in-depth for the computers and computer networks of the corporate enterprise is essential, for the data they store, transport, and process; at a time of such increasing technological dependence in critical segments of the economy, the methods of safe and secure computing must not be neglected.

The information infrastructure supporting the corporate enterprise faces a potentially devastating variety of risks and threats:

- ✍ **Access** to and **theft** of data from systems can put client **privacy, safety, and security** at risk, mean great **financial loss**, lead to **violations of civil rights**, etc.;
- ✍ **Alteration of data** or the **way data is processed** can adversely effect the client, client service, or corporate **decision process**;
- ✍ **Destruction of data** has wide-ranging implications as a lost resource in the business process;
- ✍ New threats, such as '**identity theft**' and other forms of fraud, take advantage of **operational flaws**;
- ✍ **Denial-of-service** (DOS) attacks can prevent the corporation from having use and benefit of their own computer systems and data.

Clearly, given the existing and expanding threats, the accepted metaphor of security for computers and computer networks has failed; the current operational metaphor is the principle of '**access control, basing system security and safety on access to a location, a terminal, an account** (checkpoints, boundaries). The burden of security in this metaphor is upon the automated judgment of security systems to **attempt to control the uncontrollable**--the human users of the system. Perhaps a better metaphor would provide improved means and methods for securing computers and network, a metaphor that moved the security measures from the human level down to the data and system level; this is, in fact, what a **cryptographic security** (crypto-sec) defense-in-depth metaphor provides.

Using the benefits of cryptography, the threats that target the corporate enterprise can be managed--**access or theft are prevented by cipher strength and authentication; alteration is prevented through transaction management and authentication; destruction is prevented by a different transaction model; identity issues are managed by authentication and roles; denial attacks are deflected by using authentication and filtering. Strong cryptography**, made available throughout the corporate enterprise as a fundamental element of the computers and systems, is an **enabling technology** which offers a way to construct a new security metaphor based on the defense-in-depth philosophy.

A crypto-sec system would address the threats with a shift in approach to handling security:

- ✍ '**Reader makes right**' (RMR); access controls don't work, so protect computer data and function with cryptography, where possession of a key or set of keys is essential to decipher data wrapped in one of more layer of cipher protection, or to make process requests upon the system.
- ✍ **Trust model**; trust models need to rest on cryptography, authentication, transactions, and roles.
- ✍ '**Fitness**'; security needs to be designed into the **basic functionality of the system**, not as an afterthought.

- ✍ **Transaction model**; all system interaction is transaction based, including requests for data exchange (protected under cipher) or process initiation (requests must be sent under valid authorized key, processes will be validated).
- ✍ **Roles**; all individuals have a defined role in the system, implying **authority, accountability, and risk**; proxies need to be predefined; roles are **enforced by key ownership, authentication, and audit logs**.
- ✍ **Safe fail** (option); design decisions must account for a denial attack on the system turning the cryptographic system (or loss thereof) against the security (such as a loss of the key repository in an 'all ciphered' system, thus rendering all information in the system unusable); real-time concerns, including defined **exception management**, must be regarded
- ✍ First and foremost, the corporate enterprise must accept the need for the security/safety technologies and processes; resistance or non-compliance will quickly force the failure of the system. **Non-acceptance of a crypto-sec system would commonly occur because of poor design and implementation causing unreasonable overhead or difficulty in use**; to address this, the following elements are critical:
  - **System analysis**; the corporate enterprise and work process must be accurately modeled so that the technology and processes fit the needs and requirements of the enterprise;
  - **Scalable technology**; there is a great degree of customization possible in a crypto-sec system, including variation of components, options, and approaches;
  - **Cost**; costs--be they monetary, speed of process, or of convenience--are going to occur; **nothing comes for free**, but just as alarm systems built into automobiles can be inexpensive and beneficial, so it is with crypto-sec;
  - **Ease of use**; crypto-sec does add a **layer of complexity** to using the computers and networks of the corporate enterprise; proper design of technology and process and make this less dramatic of an inconvenience while not compromising security;
  - **Reliability, availability, serviceability** (RAS); the crypto-sec system should not make the system any less reliable, nor impact on the functionality to the enterprise.

Given that **access security metaphors don't work** (proof by existence, look at the number of security incidents that are reported, look at the size of the computer security market), crypto-sec relies on a **data security model**. At a basic level, every element of the computers and networks of the enterprise needs to have access to a cipher system (probably public-key cryptography, or DES, which are the assumptions for this document); the assumption and use of a cipher for all data in the corporate enterprise provides features and benefits directly related to the mathematic principles of cryptography.

With strong cryptography, the **ciphertext** (the plaintext that has been transformed) **looks like noise**; the **only way to make the 'noise' look like something is to have the right key** (and the right key can be upward of one in tens or hundreds of millions of possibilities). Similarly, sending someone a **message not under the correct cipher key is only noise to the receiving party**. This is the foundation of the 'reader makes right' (RMR) model--the **reader must have the right key to make signal out of noise**. If all data or records in the corporate enterprise have one or more layers of cryptography wrapping them, **access security is irrelevant**--anyone can look at the file (**noise**), but only the reader can make it right (**signal**). The converse works for initiating processes or entering data into the computer or network--the request is formatted as a transaction and sent to the computer or central processor under cipher; if the cipher key used doesn't match the one expected by the computer, the transaction remains unprocessable noise. RMR systems protect **data access and privacy** by making certain that **all records are protected by at least one layer of cryptographic wrapper**; **process security** in RMR means that **authority to execute certain system processes, or issue certain orders to the system, requires the possession of the correct key(s)** to make the transaction understandable to the computer.

Cryptography also allows a certain **variable level of granularity**; a stored record can be broken down into many **fields**, and the **data in each field can be secured under a different key**. An example will help clarify this, and introduce the next concept. A medical record, for instance, has many fields--name, biographical data, medical history, orders, data from medical tests, etc. Some of these fields should only be 'readable' to certain people--a physician needs to see the entire record, while someone handling billing needs to only see a few. If each field is protected by a different key, restriction to the contents of certain fields is limited by simply not giving those who don't need access the keys to those fields.

**Roles** then, are a critical feature of crypto-sec data management, where **trust boundaries of authority and accountability are defined by the keys in your possession**. **Access to certain fields requires possession of the key for RMR; operation of certain processes, or to write to certain fields are similarly controlled** (you need the right key to encipher a command and make it understandable to the system). **Accountability** occurs because **all system interaction is based on transactions, all transactions require a minimum layered keyset use, and all transactions are logged**, thus the log reflects a detailed account of all attempts to access or process, and with an authentication attached--successful or not. This additionally allows '**transaction rollback**'--as records are lists of transactions (note that this means there are no deletions, but only a reference to a transaction handle that supercedes another), logs and records can be stepped backward and forward to watch every action by every user, and the consequence or effect. **Risk or liability management** are deeply effected by this, where it can be demonstrated who did exactly what and when, including having accessed or altered data.

Transactions and logging are critical to the 'safe fail' status of the system and network; to prevent damage by denial attacks on the cryptographic system, the default state of the storage system would need to be in cleartext, with cryptography occurring immediately above the storage system, as an element of the transport layer inside the computer and network. **A denial attack on the system might strip out the crypto-sec, but not deny the function of the system; as such attacks must originate from an authenticated source of transaction processes** inside the enterprise, **audit logs would be able to identify and isolate the source of the attack** (whereupon the keys to communicate with that point are revoked, and any further attempts at transaction are filterable noise). [Note that this sort of 'safe fail' option relies upon physical access security of the operations center (because the central storage point is 'clear'), but the actions of that limited number can be confirmed, see below.]

**Log purity**, and a secure record of all transactions, is essential; this necessitates a 'back-up' storage server which is a uni-directional receiver of traffic. Such a system could be based on 'write once, read many' (WORM) technology, adapted RAID systems, or a hardware logic and buffer system that linearized transaction activity and isolated the traffic in a unidirectional (an electronic 'airgap' by using logic gates as an 'electron gap') fashion. The log can be used for reference in a '**tell me twice**' system--comparing the normal system log and the write-once log to **confirm trust** of the internal mechanism and personnel, who can then track the complete log for anomalous, unauthorized activity. Periodic review of logs and the 'tell me twice' system is also crucial to any **exceptions** in place because of real-time concerns, where some users or domains of the enterprise require non-ciphered access, authentication override, etc. (as in the medical example, crypto-sec overhead might not conform to realtime requirements in, say, trauma care; such deliberate violation of design would be a trade-off to function, and is a weak-point in the system, one which requires that logs of such 'exception' activity receive more frequent and thorough review/audit).

Past this point, the design starts to get more technical rather than conceptual, and trade-offs need to be made based on the specifics of the situation and context. Among the features and trade-offs:

~~☞~~ unidirectional storage (WORM for 'tell me twice' redundancy, purity);

~~☞~~ regular storage (such as a RAID array; stored files may be 'safe fail' and stored in the clear, or might be ciphered, but with redundant back-ups of the key repository, at least one offsite);

- ✂ connection to ciphersystem (so all traffic across network backbone is with at least one level of encryption);
- ✂ connection to processor (centralized processing, a potential flaw, or decentralized);
  - storage of key repository (potential denial attack, but if only a dedicated hardware link into processor at this level, controllable risk, possible need for an override/key supersede);
- ✂ connection to access points (the default of all transactions working with point-to-point crypto, with authentication, or is backbone in the clear);
- ✂ access points used by personnel;
  - authentication of identity (something you have (id), something you know (password), something you are (eventual biometric but costly));
  - selection of crypto-system for performance, speed, features (including use of possible point-to-point session-to-session (even transaction-to-transaction model if the right cipher system is used, or perhaps a dynamic token system) layered ciphers to protect transport);
  - transaction model and use of ciphered/coded transaction requests; transaction granularity (are all transactions (access, process) logged; all records are transaction aggregates--no overwrites, addition only; rollback);
  - authentication and segmentation of files along role boundaries (reader makes right);
  - 'confrontation' system for periodic authentication during session

As you can see, rough conceptual designs are easy to lay out, but rapidly become dependent on the specifics of the project; this is a good thing--**no security or safety system should ever be thought of as a 'one type fits all' tool.**

## A MODEL MONEY LAUNDERING NETWORK

Money laundering, just as with any other tool of **tradecraft**, is value neutral--no moral or ethical essence itself, other than what it takes on from its use. Those who live in glass houses shouldn't throw stones--the United States, currently the largest enforcement muscle attempting to crack down on global money laundering, owes its existence to the laundering of funds from France during the Revolutionary War, and won the Cold War by laundering support to crumble the Soviet Union (Central and South America, where the effort was amateurish, sloppy, and freelance, as exposed in the Iran/Contra U.S. Senate hearings; to Afghan mujahedeen through Pakistan and global tools like BCCI; and to Poland's Solidarity movement through the Vatican). Governments are like any other social organism--when it comes to issues of security or survival, they say one thing (enforcement of independent money laundering efforts) and do another (use the tool to further policy).

Most financial transactions in an economy (other than underground economic transactions, or cash-only) create a persistent, virtual transaction 'ticket': on one side of the ticket, you can track the capital used in the transaction back to the source and probable method of earning the capital; on the other side of the ticket, you can track what the capital is used to purchase and from whom. Money laundering is any act that 'tears' the ticket, breaking the connection between the two sides--capital goes into a transaction from a source, but the recipient or reason for purchase is then unknown; or the recipient and reason are known, but the capital used has no **provenance**. In the formal terminology used by the enforcement agencies, the capital received from an illegal transaction is moved from the recipient (placement) to a laundry (layering), where it comes out with a provenance that appears legal (integration).

Law enforcement's approach to 'fighting' money laundering has been to use **checkpointing** and **pursuit**--use financial institutions and transfer mechanisms to spot transactions with questionable provenance (by amount moved during the transaction, or large numbers of sub-threshold transactions) as the virtual checkpoints, then pursue both sides of the transaction ticket to see where/who the transaction came from and where/who/what for the transaction is going to.

Industries such as the narcotics trade kick off a great deal of cash, because every time a successful transaction is completed, it **translates the mark-up/risk premium into profit**. If such money is to be used for purchasing anything outside of the underground economy or black market, and such a transaction can't be made on a cash basis, then laundering the proceeds is a necessity. The biggest problem, in fact, for the drug trade, is **overload**--too much cash money in an increasingly credit oriented society; and that overload impacts on laundering funds as well--such transactions 'stick out' in the system because of amounts per transaction with no provenance being above detectable thresholds, or because of the volume of transactions with no provenance as transaction sizes shrink to fall below reporting thresholds (the act of breaking up transaction amounts to sub-threshold levels is called structuring or 'smurfing'). The biggest benefit to the trade and laundries is that money, being **self authenticating**, is **replaceable**; money laundering is essentially buying currency for currency, with a **price for the transaction that reflects the risk premium of the transaction**.

One of the various, diverse methods used to launder currency is to move it offshore to a 'haven' with bank **secrecy** laws; the transfer may or may not trigger a checkpoint and invite pursuit (unless the physical currency is moved through smuggling, with another set of trade-offs--the potential loss of large shipments, or the increased risk entailed by attempting a great number of smaller, fractional transfers), but if the transfer occurs to the right place, pursuit cannot follow. This is the point of using 'havens'--the transfer might be detected into the haven, but once past the '**Chinese wall**,' the ticket is torn. Utilizing the funds thus 'cleaned' is still problematic; while it becomes increasingly less important to move funds back into the country of origin, those who earned the funds certainly would like to spend them.

Design of a money laundering network is an interesting exercise, the creation of a specific set of **tradedcraft**; my personal belief is that the formal intelligence community passes along tradedcraft as dogma too often, perpetuating a static, bureaucratic structure, as opposed to teaching how tradedcraft was invented and how to invent it as-needed. For the purposes of example, I'll use a drug network as my case study--one of the ways to test a design is to **force the tolerances**, see if the design fails at a potential **extreme**, and the drug trade certainly encompasses a great deal of extremes.

At a street level, the drug trade collects a great deal of cash in various denominations; the use of cash here is a primitive money laundry, since the transaction ticket exists only during the transaction (which is why at this level, the 'buy' or 'sale' use of stings is the primary enforcement method--someone has to 'swear' or evidence has to prove the existence of the transaction). For the dealer, a great deal of the cash is reinvested in supply (bumping the money up to the next step in the supply chain), but also put back into the economy on a cash basis again (this **collateral** economy from the drug trade is why there is an increasing growth in the black market--demand for goods and services to be bought on a cash, off the record, basis). The situation isn't much better at the next stage of the network--local distributors (of varying depths sub-networking based on territory size) who act as **consolidators**, they assemble an amount of cash and make the large buys, providing the **economy of scale** necessary, but also the **boundary** of the **fractioning** effort. This means that suppliers can move the product to the distributor, who is a **stable point of contact**, but don't have to be involved at the street supply level. These consolidators are the first real element in the chain needing money laundering--they need to remain a stable point because of their relationship in the network (the street has to know where to go for product, the suppliers need the **cut-out** but also the economy of having a known but small number of points of contact), so the proceeds of the trade must be usable for them. Once you get to the supplier level, such as the cartels, some of the pressure on laundering funds slacks off--it isn't for nationalistic pride that cartels tend to locate inside the primitive countries that produce the product, but because the volume of capital

buys influence, protection, and generally immunity. The dangerous monetary transactions then are from the consolidators and their local use of proceeds, as well as their need to 'repatriate' proceeds back to the suppliers in purchasing.

Moving that volume of cash is difficult--volume and weight issues aside, the loss of a large shipment is painful, while loss of smaller shipments is less painful, but as they occur more frequently, the risk of loss is greater. Think of a nice, unmarred forest--drive a heavy truck through and you leave an obvious trail of damage, but drive a smaller truck through many times and you create just as obvious a trail. So cash is 'out'--think technology. Deposit the money in some local fashion--money orders, bank accounts, other financial instruments--and move the electrons across the borders. The introduction of reporting limits was the logical law enforcement response--by creating a threshold level, it imposed a constraint problem back into the virtual world that is similar (a problem isomorph) to moving the physical volume of cash. Move a large amount of money that has no provenance, it sets off alarms; move sub-threshold amounts, and the volume gives you away. Investment in '**front**' organizations that camouflage the volume or origin of the transactions doesn't work so well any more either--accounting methods and computers can spot the traffic because of **reference models**. Take a handful of brokerages, for instance, with four running legitimate operations, and the fifth running a sideline as a laundry--the business process models derived from recording the transactions of the legitimate businesses are used as a **baseline** that shows the laundry as an **exception to the model**. Since transactions are able to be automatically monitored by computers, the judgment isn't even that difficult to automate--**flag the exception for a human to review**, let them make the final assessment.

Given the **risk/reward** and **risk/consequence** ratios, the problem isn't going to go away, but the electronic checkpoint/pursuit mechanisms have made the existing financial networks unreliable at best, or dangerous. The novel solution is to create a secondary economy (black market) with an electronic backbone. If electronic cash (ecash) or 'virtual' money come on-line in the way that some, such as the cypherpunks or people like David Chaum want it to, then the advantages of the cash economy (anonymous transactions) will formally enter the primary economy anyway (and also solve a critical issue of placement, by allowing conversion of currency 'locally' into ecash for laundering). I'm not nearly so optimistic--as much as banks themselves profit off of money laundering, they'll have to implement mechanisms for transaction mapping into any ecash system offered; remember, banks are regulated entities. Could a reliable network for money laundering be built with off-the-shelf technology currently available, and on a private basis, but that tapped into the existing economy? **Arbitrage** of international law, cryptography, and the Internet make it possible.

First, and absolutely essential, a bank or other financial institution (such as a hedge fund) must be established in a 'haven' country. Regardless of international attempts to contain, punish, or rehabilitate 'haven' countries, being an international haven for flight capital benefits the country by attracting deposited capital; poor countries become wealthy by adopting bank **secrecy** laws, and wealthy countries stay wealthy by maintaining them. The function of a haven is simple--say nothing. Pursuit of a transaction must stop at the border; **compromises of any sort will mean less value** as a haven, as the Swiss have discovered. Call the bank Hortalez & Co. (Pierre Augustin Caron de Beaumarchais, proprietor); Hortalez invests in a good computer network (see the previous example, but in this case, no data will be stored in plaintext, because 'safe' fail for a money laundry is to have all the data encrypted) and a fast connection to the Internet.

A depositor with Hortalez gets the initial capital to the haven on his or her own (a significant assumption, please note), and establishes an account. There are no papers, no photographs, no bearer certificates--the depositor is given software to calculate a public and private key; all transactions with the bank must come under cipher, and be authenticated. This is the fabled 'numbered account' but the 'number' is the keypair; transactions for the account can be made by sending a ciphered message with the order. Instructions can be left with Hortalez, such as 'pay the outstanding balance' on a credit card (issued from another offshore bank, of course), or Hortalez might offer its own card to depositors (risky, once the bank becomes known, as it will).

Take our depositor back to their business as a consolidator; they can utilize their offshore funds through the use of their credit card, or they can use Hortalez for their trade transactions in a private banking network. A set of accounts could be set up in defined denominations, and payment to another person could be not through the standard banking network or exchange of currency, but by giving the other party the keypair to an account. The new party could verify funds, and then give orders of their own, or use the keypair as if it were currency of that set denomination for their own transactions, all outside the monitored financial networks. [Yes, there are technical issues, particularly the 'double spending' issue of giving multiple copies of the same keypair; while there is much derivative work, see David Chaum's papers for the best technical solutions. I know that my first move upon receiving such a keypair would be to verify funds, and then to revoke the old keys with new ones--the process would become an automatic part of any transaction, like counting the money and making sure it isn't counterfeit currently. Also note that **reputation capital** in the underground economy is far more important than in the regular economy--knowledge of having cheated others in a deal leads others to not want to deal with you (reputation capital and '**coventry**' lists would also be banked at Hortalez) or even the 'stiff' punishment of death.] Transactions with Hortalez would soon attract scrutiny, where is why an Internet connection is essential--**anonymous** remailers. Using **chained anonymous remailers** (see Lance Cottrell's Mixmaster), contact with the bank is also laundered.

Once Hortalez has a sufficient number of clients with deposits, the system becomes an **independent** financial network. Transactions in the trade never have to move money--people transfer keypairs as payments, and the volume of transfers relying on the monitored financial system reduces down to bare minimum, with the anonymized instructions to the bank hiding in the basic **volume** of ordinary net traffic. Usage of the funds occurs through transaction orders, or standing orders to service standard financial tools (like a standard credit card issued by a reputable banking institution). Physical movement of currency would also drastically reduce; currently, all the transactions in the underground economy reduce to moving currency, just like the **reconciliation** process between banks. As the virtual money on deposit increases, use of it in transactions is low-risk, as opposed to the risks associated with moving physical currency (an interesting variation on **Gresham's Law**); the physical currency transactions would occur only to accommodate growth of the underground economy, as opposed to for every transaction. While I have only discussed this briefly and in general terms, I hope you can see why the prospect so troubles the governments of the world--it not only acts as an **enabler** for the underground economy, it also reduces tax revenues (except on consumption), and takes the monopoly power to coin/mint currency away from governments (including inflating currency, and removing the **privilege** granted to financial institutions, who can lend out multipliers (at least six to eight times) of the actual amount they have on deposit). At a fundamental level, this is why they resist **ubiquitous** access to strong encryption, and the arguments about the Four Horsemen (terrorists, drug dealers, pedophiles, organized crime) is a partial smokescreen; wide-spread adoption of this sort of system actually undermines a general key **dependency** on government power. Is this a bad thing? It depends on whether you believe in governments, or the rights of individuals to make their own choices. The joke, of course, is that the system can be built today, cheaply, and the early adopters (the black market) would benefit greatly. More importantly, it demonstrates another design testing methodology: does the concept or system **hold together under extremes in variation of assumption/variable/initial condition**, and what are the **extremes of consequence**.

---

## CONCLUSION

---

I hope that this document (and subsequent additions to it, as I add more problems isomorphs, either that I remember, run across, or hear from people) becomes a valuable tool in how you think about security, safety, and design, and that you use it as intended--to test things, to destruction if you have to, as early in the process as you can. Don't leave it to be someone else's problem or specialty--**Do It Yourself (DIY)**.

---

## ABOUT THE AUTHOR

---

With 20 years experience defense, intelligence, information operations, corporate finance, and technology development, Mr. Wilson consults on matters of organizational safety and security, critical infrastructure protection, information security and assurance, intelligence, finance, and technology for multinationals and governments in Europe, Asia, North and South America, and the Middle East. As a pioneer and acknowledged leader in the fields of infrastructural defense, information operations, open-source and next-generation intelligence, Mr. Wilson is the winner of numerous awards, including the US National Defense University's Sun Tzu Award in 1997, and the G2I Intelligence Professional Award for both 1997 and 1998. In corporate finance, he structured multi-billion dollar merger and acquisition transactions for multinational clients. As a technology inventor, his inventions and development of various technologies include: computer security systems, anti-viral computer hardware, cryptographic methods, agent-based modeling, three-dimensional visualization and interfaces, and massively-parallel, massively-distributed processing systems. Mr. Wilson's educational background is in system theory, cybernetics, and general semantics, PERL (political science, economics, rhetoric, law), and physics. He can be contacted via email at [info@metatempo.com](mailto:info@metatempo.com).

NOTE: This is a re-release of this paper which was published in 1997 by 7Pillars Partners. Permission was granted by 7Pillars Partners for this re-release. 7Pillars and Michael Wilson retain all copyright and intellectual property related to this paper.