Issue #12 - July/August 1995

Cybertek

The Cyberpunk Technical Journal

Technology, Security, Self-Reliance

Published by OCL/Magnitude, P.O. Box 64, Brewster, NY 10509

"A people who mean to be their own governors must arm themselves with the power knowledge gives."
- James Madison

The Cheesebox

by Thomas Icom

Background

The cheesebox turns two phone numbers into a loop line. What this enabled one to do was communicate with another party without having to disclose either party's phone number. The first party would call into line one, the second party would call into line two, and the cheesebox would connect the two lines together, enabling the two parties to communicate.

Other variations of the cheesebox, often called "CF (call forwarding) Boxes", or "Diverter Boxes" enabled one to call line one and receive line two's dialtone. These boxes are still available commercially; mated with an autodialer for use in a person's place of business to reroute calls to an answering service after hours.

Implementation

This version of the cheesebox is based around the Parallax BASIC Stamp. This microcontroller was chosen due to its small size, extreme versatility, and inexpensive price. The use of a micro-controller also enables one to use a minimal amount of support hardware, as control functions are handled via software.

There are two versions of software for this device. The first listing is designed to go off-hook as soon as a ring is detected on the primary (incoming) line. The second listing waits 30 seconds (The time can actually be any length up to 18 hours. That's one of the nice things about using a microcontroller.) after hearing an initial ring; at which time it will then pick up on the first ring of the next incoming call.

After detecting a ring, the device picks up the primary and secondary (outgoing) line. If the secondary line is not in use, one will receive the secondary line's dial-tone. If the secondary line is ringing at the time of seizure, the device will "answer" it. To the caller on the secondary line, this would sound like a regular phone call (alleviating some suspicion if instead the caller was just told to dial the number and wait in silence; thus indicating potential cheesebox usage). If the secondary line was in use, the caller into the primary line would be thrown into the conversation occurring on the secondary line. While this might prove to be interesting for PSYOP purposes, the use of this device in its current configuration for surveillance would be a poor choice, as the audio path would be two-way, and cheesebox picking up the secondary line would be as detectable as if someone picked up a regular extension (ie. a "click" would most likely be heard, and the line voltage would drop).

Once the Stamp picks up the phone, line voltage is used to latch open the two 12V line relays. The Stamp then goes back to waiting for a ring detect again. When the caller on the primary line hangs up, the line voltage will drop to zero and the relays will unlatch. The cheesebox is ready for another call.

When the Stamp is in its normal state, it draws 2 milliamps of current. When it picks up the phone, this goes up to 22 mA for about three-quarters a second. Under those circumstances, a 9V 600 mAh battery will last somewhere around ten to twelve days. This is extended by using the Stamp's sleep feature so that the Stamp only checks for a ring roughly three times a second;

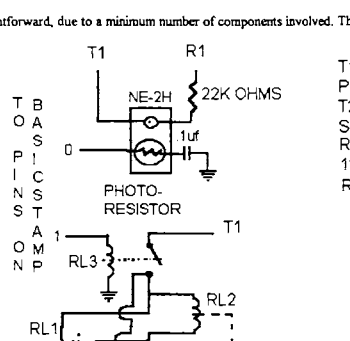
as opposed to a thousand times a second. When in sleep mode the current draw is only 20 uA (0.020 mA). This should extend the battery life to somewhere between twenty to thirty days, depending on use.

Hardware Construction

The first thing you should do is read tbe manual that came with your BASIC Stamp programming package. It's full of useful information you will need to know in order to successfully complete this project.

Hardware construction is pretty straightforward, due to a minimum number of components involved. The following will be required:

1 BASIC Stamp I Module with carrier board (available from Parallax)
1 BASIC Stamp Programming Package (Parallax)
1 Ring Detector Module, which consists of:
  1 NE-2H Neon Lamp (Radio Shack #272-1102)
  1 22K Ohm Resistor (Radio Shack 271-1128)
  1 Photocell (exact type not important. I used one from Radio Shack's #276-1657 package.)
1 .1 uf Capacitor (Radio Shack #272-135)
1 5V SPST Reed Relay (Radio Shack #275-232)
2 12V SPST Reed relays (Radio Shack #275-233)
1 1:1 600 Ohm Isolation Transformer (Radio Shack #273-1374)
1 560 Ohm Resistor (Radio Shack #271-1116)
Hookup Wire
Electrical Tape
Electronic Tools (Soldering Iron, Solder, etc.)
4 Alligator Clips
1 Decent capacity 9V battery, preferably rechargable (such as the 600 mAh Radio Shack #23-229)



The BASIC Stamp and Programming package can be ordered from:

Parallax
3805 Atherton Rd. #102
Rocklin, CA 95765
916-624-8333
FAX: 916-624-8003
BBS: 916-624-7101
FTP: ftp.parallaxinc.com
WWW: http://www.parallaxinc.com

This should all fit on the prototyping area of the Stamp's carrier board, although some care should be taken as to placement. The one step that should be paid attention to is the ring detector. This consists of the neon bulb (with it's dropping resistor) and photocell.

Take a length of electrical tape and wrap the photocell and neon bulb together, taking care that the leads of each component don't touch. You want to make this as light-proof as possible, a second layer/piece might be necessary. When this

is completed, attach the dropping resistor to one of the neon bulb's leads and attach the neon bulb/resistor combination to the phone line. Attach an ohm meter to the leads of the photocell. You should get some high reading. Now ring your phone and watch the ohm meter. The reading should go down significantly. If it does, then your device works. If not, check the construction and try again. The exact readings are unimportant, you just have to get a high reading when it's idle and a low reading when it detects a ring.

Once you have the ring detector working, you can attach it to the Stamp according to the schematic and calibrate it. Load up your programming software, attach and power up the Stamp, enter the editor and press Alt-P. When asked for the pin, input "0" (That's the pin you connected it to.) Hook up the ring detector to the phone line, and while the calibration routine is running; ring your phone. Write down the scale value that appears, you will need to put it in the source code at the appropriate place. (You should understand once you become familiar with the Stamp and see the source code.)

After the hardware construction phase is completed, load up your programming software, and put one of the following pieces of source code in the stamp.

Software

Pick Up on First Ring Version
CHEESE1.BAS:

```
start:  goto wait
pickup: high 1
        pause 1000
        low 1
        goto start
wait:   pot 0,xxx,b0    'xxx=The # received during calibration
        if b0>0 then pickup
        nap 4
        goto wait
```

Ring Once and Then Call Again Version
CHEESE2.BAS

```
start:  goto wait
pickup: high 1
        pause 1000
        low 1
        goto start
wait:   pot 0,xxx,b0    'xxx=The # received during calibratio
        if b0>0 then window
        nap 4
        goto wait
window: sleep 30
secheck: pot 0,xxx,b0   'See earlier pot command.
         if b0>0 then pickup
         nap 4
         goto secheck
```

Operation

Operation is pretty straightforward. A nine volt battery is attached and the box is hooked up to two phone lines. The primary wires will be attached to the incoming line, and the secondary wires to the outgoing. When a call is made into the primary line, the caller will be switched into the secondary. When the caller hangs up, the cheesebox resets itself and waits for another call.

Ω

The Essence of Warfare

by **Atreides**
The Nemesis Group

Heraclitus noted that a man cannot walk in the same river twice, for it was not the same river, and be was not the same man. Less eloquently, things change. It stands to reason that conflict, at once the driving force for change, the method of change, and the fall-out from change, would itself change in nature over time. As things change, and we are able to observe more of it, certain patterns begin to arise; distance, in space and time, certainly lends perspective.

Once Man thought the Earth was the center of the Universe; then Galileo worked out a theory of motion, and paid tbe price; Newton comes along, and given some room for contemplation, generalizes a number of principles; Einstein catches some flaws and postulates an even more generalized set of theories. We all stand on the shoulders of Giants.

No surprise, then, that some basic concepts behind the Art or Science of War are becoming more evident as we once again transform our ways of thinking on the subject.

Approaches to conflict in the world fall into a four-quadrant grid, passive-active on one axis, defense-offense on the other. Passive defense stems from the assumption that a situation is 'friendly,' while active defense assumes 'hostile.' American activities tend to fall into this first category, while tbose of the Cold War Soviet Union fell into the later. Passive defense is lethal--no wonder that America has found itself playing catch-up on every conflict it has ever engaged in. The inherent danger of active defense is seen in the fall of the Warsaw Pact and sponsor; total collapse from exhaustion as they actively tilted every windmill.

The other grid half is the realm of the active and passive use of force. Active offense, primarily the unnecessary bifurcation into attrition and manoeuvre warfare, is an area of excellence for the United States. Passive offense is an area that eludes the military establishment, although, as I will explain, this isn't necessary with a deeper understanding of what conflict is about.

Life is the struggle for the free energy in a system; even the most basic organisms are primarily 'concerned' with metabolism and reproduction. As a political economy progresses and evolves, interesting things happen, as you would expect in any system where complexity can be measured by the combinatorial of interaction of the aggregate sub-systems. Political economies (PE), social structures if you will, can be defined by the depth of what can be called 'dependency infrastructure,' or the 'value add' chain.

The most basic political economy is that of the Agrarian society, The Age of Bread. Such social structures have a very short 'material' value chain (phases in a process where the receiver of the process experiences a net gain in value or performance because of the prior process), and a short 'informational' value chain. For example, the material value chain of hunter-gatherers is minimal, just the raw labour involved in the acts of hunting and gathering, and the informational value chain is food stuff identification and processing knowledge. Slightly more complex is a feudal society, where already the material-based labour component was being replaced with the informational--blacksmithing and tack to create plows, knowledge of planting seasons, milling grain for bread, animal husbandry. This period is still preoccupied in the struggle for the basics of life--food, shelter, warmth, procreation (Maslow's Hierarchy); resource, labour, and capital are King (usually quite literally, trapped in a zero-sum game, hierarchical political economy).

The next phase of development is the Industrial Age, The Age of Mass Production. This phase has long value chains in material resource (components to build components to build components...; tools to build tools to build tools...), and a steadily growing value chain in informationals. Additionally, considerable effort is dedicated to the social contract, another example of spontaneous order, which allows the complexities of a political economy to function. The human species, not content to let such systems be self-regulating, has wasted enormous resource in the attempt to govern (in a cybernetic sense) the process, not realizing that where there is free competition, there is no dependency, something most groups claim to desire.

The current phase of development is what has been termed the Information Age, the Age of Patents. Material value chains are beginning to die back, while the informational value chain is increasing; this reflects the situation that embodied thoughts can have value (and in fact are replacing the resource-labour-capital triad), while still being dependent upon the infrastructure. Western civilizations, the most advanced of this phase, are fumbling with the new informational value chain that progresses data into information into knowledge into wisdom; most effort actually goes into simple shuttling of raw data and a little

information from here to there. The social contract is more confused than ever; specialization has been forced by the complexities of getting to this phase, yet most of the critical basis for interaction is being undermined. It is still increasingly an age of positive-sum games, heterarchies, etc.

Interestingly, extrapolation of this trend leads to a further or complete decay in the material value chain, possibly because of advances in space exploration or nanotechnology. We'll have to wait to get there-then to see which it is.

Now to return to conflict. In the Agrarian Phase, direct control of the means of production through possession was necessary; from this phase we have centuries of examples of 'conventional' warfare, attrition style. As advances were made into the Industrial Age, devastation of the dependency infrastructure was no longer a viable option--what was broken couldn't work for the winner's benefit. This led to progress in manoeuvre warfare, where control became important, rather than devastation. Other than a decidedly significant side-trip because of atomic and then nuclear weapons, this remains the guiding principle of modern warfare. In fact, it demonstrates (satisfying the correspondence principle as well) a more fundamental nature of 'warfare' oriented around the dependency infrastructure (DI):

- Conventional warfare seeks victory by overwhelming or through forcing a failure of the opposition's DI.
- Manoeuvre warfare seeks victory by taking control of key elements of the opposition's DI, essentially imparting control.
- Guerrilla warfare orients around opportunistic attacks on the opposition's DI, making the energy cost of conflict too great to maintain.
- Political warfare is control of the members of a political economy through (establishment and) control of a DI, coupled with media manipulation, propaganda.
- Terrorism is a case of actions taken against the social contract to attract media attention to a conflict when the media is (perceived to be) controlled by the opposition.

A dependency infrastructure is composed of widely varied elements of the social contract of the political economy--command-control bodies, social services, education, the workings of an economy, communication systems, spiritual leaders, anything that supports the value chain of the phase.

Warfare, then, is about the control of the dependency infrastructure; some forms of warfare need not require a single shot to be fired, instead seeking victory through establishing control of the dependency infrastructure. This cognitive tool explains many things:

- Gandhi was successful in large part by his demonstration that the infrastructure of the raj was in the control of the Indian people, and they reasserted themselves in this fashion. Other strategies of Gandhi bear study, including his self-creation as a media symbol and deliberate infliction of harm upon that symbol as a method of war, whether through his being arrested, or fasting to the point of personal bodily harm.
- The problem of Iraq for the West, post-Gulf War, is that their dependency infrastructure was left intact, and in the hands of Saddam Hussein. This does not question the validity of the conflict itself, which has been claimed to be in the 'national interest.' The rule of thumb to see if something is a national interest? Does it have an effect on your dependency infrastructure to a dangerous degree. Any singular control of significant OPEC resources can be viewed as a weapon in the making.
- Social unrest occurs because of a failure of the dependency infrastructure for those suspended and dependent inside it; riots are a symptom of this disease, by people who suffer from a cultural disease we have no name for.-- The odd relationship the U.S. has with terror; access to the free media market has become important to support for a cause, while the blind eye the U.S. turns on certain issues makes them a target. Any group who feels a media bias on an issue, Palestinians versus Zionist occupation, Ireland versus United Kingdom rule for example, will be caught trying to have it both ways.
- The problems the U.S. faced in Viet Nam, such as the inability to control a dependency infrastructure with air strikes, or the total corruption of the allied infrastructure, driving anyone adversely effected to the alternative infrastructure supplied by the Viet Cong and NVA.

It also suggests a new form of warfare where victory comes from the establishment of alternative dependency infrastructures in a political economy, in conjunction with propaganda efforts (which would be useful in the Former Soviet Union, Central and South America, or North Africa for example). Let me also add that it is going to be a serious failing in areas such as Gaza/West Bank where no infrastructural development is being undertaken, the greatest threat to peace in the region.

Following this chain of reasoning, even new areas of thought on conflict make sense, such as the special case of information warfare--at one end it can be used as a weapon of mass destruction (WMD) just as nuclear, chemical, and biological weapons which overwhelm the dependency infrastructure of an opponent, and at the other end it can be used in guerrilla, terror, or political warfare to selectively destroy or surreptitiously control the dependency infrastructure. Seen on these terms, it makes perfect sense in terms of doctrine; it also explains why it is an increasing and soon to be critical threat to the nations of the West.

Conflict this far down the line is not getting any easier. To understand what is occurring in Bosnia or Somalia, you have to put them in their context; to understand future conflicts, with guerrillas, terrorists, propaganda, hackers, cyberpunks, et al, we will have to search for the basic essence of conflict--because only by understanding those basic principles will we be able to prevent the world from falling apart around us, or at least not be caught out by it when it does.

Ω

Alternative News Gathering Techniques

by Thomas Icom

What never ceases to amaze and disgust me is with the extensive means we have in this country for the dissemination of information, I find that it is more difficult to get real news about matters regarding personal survival, than it is to find out the latest fad in Hollywierd. I don't know whether it's because the American people have sunken to the lowest common denominator, or if it's because New World Order advocates in the media are deliberately trying to keep the people ignorant to further their aims

James Madison once said "A people who mean to be their own governors must arm themselves with the power knowledge gives." With that adage in mind, it would make perfect sense for the totalitarians to keep their potential subjects in the dark, as it would make their ascension to power easier. Whatever the reason, the result of this situation is that people into personal security and self-reliance have to make a little extra effort to stay informed.

Ironically enough, one of the best places for certain types of news and intelligence is the idiot box (TV). If you have cable, you probably have access to a network called "CSPAN". CSPAN is a public affairs network that feeds the activity of the senate and house of representatives right into your home without any commentary attached. When the house and senate aren't in session, they cover press conferences and meetings of public organizations. Not only does CSPAN let you see what your "elected representatives" are up to; it lets you know who your friends and enemies are. The latter can also be said of monitoring network-TV news and "popular shows". If you can stomach it, watching network-TV will also give you a practical education on enemy psychological warfare techniques. Such an education is necessary in order to implement effective counter-measures.

One of the "better" networks for news is CNN. Since all they do is news, they will report on things that will be missed by the other networks. The drawback to CNN is that you need to have Cable TV in order to get it. For those in areas without cable,I would suggest checking the FM and AM broadcast bands for an all-news station. Some news radio stations do rebroadcast CNN's audio.

The shortwave bands still remain one of the best sources for alternative news information. Despite their increasingly socialistic leanings, you can still receive better quality news from overseas stations such as the BBC and Radio Duestche Welle than you can from CBS, NBC, and ABC. More American stations are also coming on the air, a radical departure from the days when the VOA (Voice of America, a government run station) was this country's only voice on shortwave. These American stations, particularly WWCR, provide an excellent amount of alternative news and current affairs commentary in their programming. Specific frequencies for a shortwave broadcaster change periodically. A current issue of Popular Communications or Monitoring Times magazine will provide you with specific frequencies and times of broadcast, but if you just want to tune through the bands and look around, the most common frequencies (in Khz.) used for shortwave broadcasts are:

5950-6200	9500-9775	7100-7300	11700-11975
15100-15450	17700-17900	21450-21750	25600-26100

The frequencies below 10000 Khz. are better for nighttime reception; while those above 10000 Khz. are better for reception during the day.

Small press publications, colloquially known as "underground newspapers" or "'zines" are more popular today than ever with the advent of desktop publishing systems and personal copiers. I personally believe that the advent of low-cost personal computer-based publishing systems was one of the greatest things ever to happen to the cause of freedom! The reason behind this belief is that now anyone with a little spare cash and a cause can become their own press. So, what was once the domain of big corporations is now the domain of anyone who wants it!

There are too many excellent alternative press periodicals out there to list. I'm going to list a few of my favorites, but for more **I strongly suggest you subscribe to Factsheet Five**. Factsheet Five is a 'zine whose entire purpose is reviewing other 'zines. If you're looking for it, you'll find it in Factsheet Five. Factsheet Five is generally available at your local Barnes & Noble bookstore, or you can get it via mail.

Still talking about computers, another excellent alternative news gathering and dissemination technique are computer bulletin board systems (BBSes). A BBS is a computer system that is set up by a private individual for the purpose of other people calling into it to leave public messages private messages (e-mail) to other users, and public-domain (free distribution) software. Some of these BBSes are networked; which means that you can make a local call to a nearby BBS, post a message, and have it distributed across the world in 24 hours. Every semi-populated area has a local BBS that is part of "Fidonet", the largest of the BBS networks. Most BBSes are free to use; with you just paying for the cost of the phone call; although some solicit donations to help offset the cost of running the system.

All of this is done with your computer and a device called a "modem"; which interfaces your computer system to the phone lines. Modems and BBSes are another great invention for cyber-libertarians and other dangerous types who are into freedom. If you want to say something, just jump on your local Fidonet node and within a day or two your opinion will reach the opposite coast and everywhere in-between.

It's easier to get in the BBS scene than it is to get into desktop publishing. All you need is a computer, a modem, and a terminal program to make the two work together. You don't even need a "state-of-the-art" system to do all of this, as the standards used for communications are universal between the various computer systems.

Again there are too many BBS systems out there to mention them all, but for now I'll mention the official Cybertek BBS; RuneStone BBS, (203)-832-8441. When asked for the "newuser password" enter the word: CYBERDECK.

Going beyond BBSes, we have the Internet. The Internet has come a long way since its inception. It eliminates the disadvantages of BBSing (large LD phone bills and a relatively small audience) while retaining all the advantages. There is already a ton of information out there available on the Internet, so I won't go into any major detail on it. Nevertheless check it out. It's a very powerful tool.

In regards to news in your local area, the best thing I've seen is a "scanner radio". With one of these tuned to your police and fire frequencies, you'll get a first-hand report of events in your local area. While some places are beginning to scramble their radio transmissions, overall the practice isn't common. It might also pay to attend your local town-board meetings, as this will also give you a first-hand look at how well, or poorly, your community leaders are doing.

The entire shortwave frequency spectrum (1 Mhz. - 30 Mhz.), as well as the AM and FM broadcast bands will probably become very useful in the event of a hostile takeover of the United States Government, whether it's from an internal problem, or an external power trying to take over. In such a case, freedom fighters with the background and equipment could set up underground broadcast stations to help the resistance effort. This will be more prominent on the shortwave bands because the equipment is easier to obtain, and due to the nature of the band, it is more difficult to use radio direction finding techniques to track down an "illegal" transmitter.

Also of interest to survivalists is the Emergency Broadcast System. This is run by the mostly non-existent Emergency Management Authorities to provide official news and instructions in the event of a national emergency. It is one of the holdovers from the 1960s Civil Defense Program, and unless you live near a place such as a Dam or Nuclear Power Plant, there isn't much to the Emergency Broadcast System other than the fact it exists. However, if you have a spare AM/FM radio, or TV it might prove at least interesting to listen too, just to see what little the government informs you off, or instructs you to do. In the event of an actual emergency, I suggest programming the areas public safety frequencies in your scanner, as you

will probably hear more information over them. You might also want to tune around the ham radio bands in the event of a nationwide emergency. Many hams are involved in disaster relief services such as Red Cross and RACES (Radio Amateur Civil Emergency Services). Being a ham operator myself, I can tell you that a lot of infogoes over these frequencies, both official and unofficial. Common frequencies are:

3500 - 4000 Khz. (80 Meter)	7000-7300 Khz. (40 Meter)	14000-14350 Khz. (20 Meter)
21000 - 21450 Khz. (15 Meter)	28000-29700 Khz. (10 Meter)	144-148 Mhz. (2 Meter)

The frequencies labeled in Khz. are shortwave frequencies, and offer worldwide coverage. The 80 and 40 Meter bands offer better coverage at night. The 20 Meter band offers decent coverage around the clock. The 15 and 10 Meter bands are best during the day. The 2 Meter band is a local coverage band which is useful for finding out news regarding your local area. Also potentially useful to listen too would be the CB band. Everyone has at least one CB which makes it a good community "jungle telegraph".

The above is just a small sampling of radio frequencies that might yield useful information. You will also want to read Thomas Roach's excellent book The Hobbyists Guide to COMINT Collection and Analysis which was reviewed in Issue #10.

Small Press Periodicals Worth Checking Out

2600 Magazine: The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953
516-751-2600
Good magazine covering computer and phone security. You'll also want to acquire the eleven years worth of back issues, as they make great reference material.
$18/year

Factsheet Five
P.O. Box 170099
San Francisco, CA 94117-0099
$20/year
Reviews other small press 'zines. Excellent source for those of you wanting to expand your sources of alternative press periodicals.

Gray Areas
P.O. Box 808
Broomhall, PA 19008-0808
$23/year
A highly recommended magazine that covers "the gray areas of Life" - 'nuff said! Netta Gilboa, the editor and poublisher, is one of the few people I've seen who has given the computer underground an objective and realtively unbaised look, and let them have their own unedited voice, despite all the shit that certain STUPID people in that community have given her. (Those who disagree should compare her coverage of the community with that of the establishment media.) That fact alone gets her my support.

U.S. Militia - "The Only Magazine For Community Defense"
Kurt Saxon's excellent periodical version of The Poor Man's James Bond.
$35/year

Shoestring Entrepreneur
Another excellent self-sufficency periodical by KurtSaxon. This one is geared towards learning a trade and using it to go intobusiness for yourself.
$15/year

Kurt's periodicals are available from:
Atlan Formularies
P.O. Box 95

Alpena, AR 72611
(501)-437-2999

Iron Feather Journal
c/o Stevyn
P.O. Box 1905
Boulder, CO 80306
$5 for current issue
This techno-anarcho 'zine is another favorite of mine. I think Jerod Pore put it eloquently and accurately in Factsheet Five #52 when he said that *"Iron Feather Journal is the Anarchist's Cookbook of the '90s, without all the bogus data that would get you killed."*

Ω

Telecom Remote Control
Part 1: Introduction
by Thomas Icom

The use of the telecommunications network for remote control purposes has a number of advantages. It's world-wide in scope, allowing you to reliably activate remote control devices from anywhere in the world that has phone service to anywhere in the world that has phone service. While you might have problems in an underdeveloped third-world country, you won't anywhere else.

A number of signalling methods are available for telecom R/C applications. The first and easiest is a simple ring detect. The phone rings and the device activates. This does have the disadvantage of lacking control; as any ringing after installation will activate the device. To help alleviate this problem, you can add a counting circuit so that the device isn't activated until a certain number of rings have occurred. Another way is to adjunct the ring detector with a timer switch, so a certain amount of time must elapse before the ring detector becomes active. A benefit to ring detection is that the caller isn't billed as the pbone isn't answered.

You can also have an auto-answer module with a DTMF decoder. In this instance, the device will be activated upon receiving the proper sequence of DTMF tones.

Dual-Tone Multifrequency (DTMF) tones, or "touch-tones" are the most common signalling method for R/C applications. DTMF signalling was originally designed as a means for quicker dialing for telephone subscribers. It's versatility has lent itself to other signalling uses. The wide availability of DTMF equipment has made it a common signalling method for accessing voice mail, interactive phone systems (such as the ones banks use for customers to receive their account information), remote dial-ins for PBXes, WATS extenders, and answering machines, and R/C devices.

The wide availability of DTMF equipment is also a security disadvantage. Your R/C device is vulnerable to anybody with a touch-tone phone and a little time on their hands. You can counteract this somewhat by making security codes longer, but this will lower efficiency by increasing system usage time, and might present a memory obstacle to the systems' users; who then might violate a basic security measure to assist them in accessing the system. (i.e. Never write anything down.)

Discrete single or dual tone signalling can also be used. Since the tone signals would be proprietary, security would be increased. The actual frequencies could be changed at will for an even greater increase in security.

To this end, many DTMF encoders and decoders can be modified to transmit and receive signals which are of a different frequency than those used for DTMF signalling. This is done by changing the reference crystal hooked to the device's encoder or decoder IC. A common example of this is the replacement of the crystal in a particular model of DTMF dialer in order to generate coin tones for toll fraud purposes. In our case however, a DTMF dialer is modified to satisfy a legitimate security need for a telecommunications based remote control application.

The ultimate method in security and versatility would be a microcontroller and an auto-answer modem. You could require a password to access the system, and then additional passwords to activate various devices. The modem could require any number of rings to answer. Finally, the micro controller could be programed to only accept certain commands at certain times.

The use of caller ID (CID) in telecom R/C devices adds another dimension to security. Devices can be set to activate only if called by a certain number. It would be no major feat to wire up an and-gate to certain segments in a CID box's display, so a control line goes high when a certain number calls. The caller would also not be billed for the call, as the CID data is sent during the ringing cycle.

The construction of devices for telecom R/C is easy due to the wide availability of off the shelf equipment that is either readily modifiable, or adaptable to "kit bashing". You should be able to assemble a plethora of devices after visiting a few tag sales, flea markets, surplus stores, pawn shops, or their local Radio Shack. By going that route one will be able to keep costs down. Even in an extreme condition you can acquire the necessary materials from a department store, but why spend $30 for a new piece of equipment you're going to take apart when you can spend only $5-$10?

In Part 2, I will present some telecommunications remote control projects and applications

Ω

The Precipice Problem: A Guide to the Destabilization of Western Civilization

by **Atreides**
The Nemesis Group

No one but a sage can utilize espionage... —Sun-Tzu

1.0 Introduction and Background

It has rapidly become possible for a small group of knowledgeable and skilled individuals to create chaos, wreak havoc, destabilize, and potentially destroy what is currently referred to as 'Western Civilization.'

Once it was possible to accomplish such goals through the removal, by various means, of the ruler of the dominant country of the 'Empire.' Rendering unto Caesar what is due him becomes moot if Caesar has been eliminated. However, the swift rise of democratized countries as the dominant powers of the world has added a certain amount of cultural resiliency, making such a manoeuvre obsolete. In its stead has arisen a new, more virulent, form of attack--such empires are now built upon economic strength (Gross National Product [GNP] is the most critical factor to be taken into account, even regarding military strength, witness the resolution of the Cold War in favor of the U.S. and NATO forces over the Soviets and Warsaw pact forces strictly via extended economic, as opposed to military or pure ideological, conflict), and such strength can be swiftly negated, as it relies upon technology. Caesar could always be quickly replaced, an economy cannot be.

Negation of an economy, and hence a country dependent upon it, is accomplished through the skilled manipulation and usage of technology in conjunction with the exploitation of the flaws--inherent, accidental, or deliberate--of a technology-based society.

An economic maxim of obvious truth is that control of the means of production implies control of a society. While the maxim has remained the same, the factors comprising it have evolved--the means of production have changed from the factory worker to the 'knowledge' worker and electricity has transformed from a unit of work to a unit of information, but then again, so has everything else (money, etc.).

Termed the Information Age of Western Civilization, it has given new possibilities and benefits to the citizens of the West, although it has left them in a completely exposed position as far as long term viability is concerned. It has created new avenues for dominance and manipulation [which is why the Japanese are trying to dominate through technology], and ultimately, the power to destroy is the power to control; technology is a sword which cuts both ways, an Achilles' Heel of the West.

'Western Civilization,' as it has evolved and currently stands, is defined by its advanced technology. Such technology is a recent development, historically speaking, and thus the window of opportunity for such an economic attack has only just opened. The combination of such 'newness' with the almost immediate dependence upon the usage of technology has created the most significantly vulnerable area of attack in the history of the culture.

The maxim 'those who do not study history are doomed to repeat it' once again plays truly in this case. For example, essentially every culture has built bridges; in fact, bridge building, masonry, goes back into the depths of time. Yet every culture, when learning to build bridges has made numerous mistakes, usually costing numerous human lives. This is the price associated with learning; tracking these developments eventually leads to the science of engineering.

The history of engineering, which builds bridges, ships, or airplanes is that of one disaster after another, but always something that can be learned from. What develops is an engineering 'rigor': performing testing and extensive analysis, and not trusting that something can be reliably done until you have actually done it.

Yet when it comes to technology, it seems that reason flew out the window. Even though you can't test code the way you can test metal or concrete's material strength, even though there are one-of-a-kind systems that were never intended to be doing the job they are forced to do, the West has passed over complete control of the critical functions holding their society together to the unreliable machines. Why? Because it was convenient, and some things (such as the large volume of phone traffic or banking transactions) just weren't possible otherwise.

The individuals 'in the know' on these problems are perfectly well aware that they can't verify the function of their technology, can't be certain that it does what they say it does reliably, and have no way of being positive that it doesn't do more than it says it does; they can't even guarantee 'bugless' code, let alone 'hardened' systems. But if nobody says that the Emperor has no clothes, maybe no one will notice. Perhaps a good example is that of the 'rules of the road': everyone knows that driving can be dangerous, yet sane drivers in sane situations will obey the common courtesies of driving (staying in the proper lane, stopping at lights and signs) even in the absence of an enforcing officer. Why? Because the potential for danger to life and limb is greater once you 'break' the rules. Here we have a similar situation--if everybody behaves and treats the systems very nicely, then they will continue to function as intended; stray outside the decorum of good behavior, and you have a disaster on your hands.

But that still leaves a vulnerable situation, an accident waiting to happen, or an opportunity looking for someone to take advantage of it if they know what they are doing.

A further note--it is only getting worse (or easier, depending on your viewpoint). Every day, more is automated, more network connections are established, more people, places, and things become dependent upon technology. Because of this, a society that is already standing on a Precipice becomes even more unsteady, stands on less firm ground, waiting to slip. Or be pushed. Remember, this isn't a case of 'going downhill'--it's a case of dropping off a steep cliff.

The advancing policies of both industry and government are actually increasing the risk the West is in; for example:

The creation of various standards (whether de facto through market clout or through imposition) does incredible damage; the major limiting factor to disease in humans, crops, and livestock has been the heterogeneous nature of the population; reduction of the technology arena to a homogeneous environment (for instance, with a major dominant hardware platform and operating system such as is occurring) only paves the way for the wreckers;

Almost every group in the West with some interest in computers, communications, consumer products, or technology in general is pushing for the creation of a 'super datahighway' or greater connectivity; if the dreamers have their way, everybody will be connected by a tangled web of twisted pair, coaxial cable, optical fiber, microwave, radio, and even local infrared.

This bestows great access upon John Doe, but it also builds an irrevocable dependence in the economy, the way people do business, and the way the culture works; even though technology has become wide scale in the financial community only within the last decade, groups such as banks, credit suppliers, or stock brokers would be helpless without it. Now extend that to John Doe, and see how little cash money he carries, how dependent upon 'plastic' he is, and how much chaos his life will be if everything crashes.

In addition to the economic functions that advocates wish to be turned over to the new systems, there are numerous social ones--from medical care to electoral voting; the potential damage that will eventually be able to be done is beyond calculation.

No large scale organization (from 'Empire' to the human body) can exist without a fundamental bedrock of communication and infrastructure, yet we see that the expansion of the existing 'Empire' has foundations built upon sand, and worse still, we're

busily at work pulling up the old granite foundation and replacing it with sandstone, all in the interest of renovation. Madness, indeed.

2.0 Operational Overview

Critical potential targets of the problem are the infrastructure of the economy. Much like a circulatory system in a human body, which provides oxygen and nourishment to the various parts, the infrastructure of an economy acts similarly. Destruction or damage to it on a massive scale causes irrecoverable harm to the basic structure and integrity of the economy. Operational techniques to carry out the 'hostile' outlined program are briefly discussed in the 'Informational' subsection of the 'NCBI' section later in this document.

Let's assume an adversary and see what they could do:

2.1 Telephone Communications

Conventional communications, including voice conversations, fax, data, etc. are providing absolutely critical support for the West--without them, little could occur owing to the dependence upon the frantic 'societal pace' and sizable and diverse territory covered. This dependence includes all transactions--domestic, international, government-- yet even the most sophisticated of communication set-ups is an AT&T 3B2 UNIX minicomputer with a telephone backplane hypernetworked together as an electronic switching system. Such systems are trivially simply to disable, commonly causing cascading malfunctions on their own.

Other component parts of the communications grid are also easy targets, such as the microwave transceivers, or satellites themselves, which can be brought back down to the ground through reprogramming of their on-board but ground-controlled attitude jets (simple to do if one can grab the legitimate equipment and software used to do such). The emergency 911 and 911E systems could also be specifically targeted in advance to contribute to the impact of the impending chaos.

Disabling the telephone system also, as collateral damage, disables all ancillary services which depend on communications via the system: police, fire, emergency medical care, alarms of all kind but primarily of security systems, power control, water, sewage regulation, etc.

Take as a case study the mishap which occurred in New York on Martin Luther King Jr. Day only a few years ago. Cascading failures of the switching systems caused communications havoc for the 'long lines' of the Eastern Seaboard. It is still inconclusive whether outside interference contributed to the failure, but the cost was enormous, even on a Federal holiday.

2.2 Power

Power generation plants are manually controlled, thus making them fairly resistant to tampering and manipulation from informational warfare attacks. This is primarily due to their having been designed and constructed during a period in which fail-safes were taken more seriously, as well as the potential for civil unrest, coupled with the fact that most are pre-'information age'. However, the power distribution and regulation systems are electronically controlled, making them potential targets.

If a hostile party wished to indulge in physical operations to augment the informational warfare, American power generation targets are 'easy pickings' from that stand-point. Security designs are remedial, coupled with poor implementation. For example, one nuclear power plant TNG principals analyzed had no 'forcing factors' requiring a confrontation with security systems or forces to destroy the plant; security is geared to fit regulation requirements and keep protesters away, rather than prevent an actual attack. The security precautions also seemed, absurdly enough, to take for granted that an attack would be aimed at taking control of the plant, rather than simply destroying it (which could be accomplished from outside the security perimeter with three people and costing less than $10,000 [U.S. 1993 dollars]).

2.3 Financial

Making direct attacks on the financial community that the West depends upon is quite easy--the emphasis in this community, even when security was considered worthwhile (security does not contribute to the 'bottom line' of quarterly profit and loss statements, and is thusly considered a waste of capital), it has been focused on prevention of theft, not against malicious attack. Even then, theft is covered by insurance, and the amount stolen comes nowhere near the amount necessary to retrofit more security into the systems; it is considered acceptable loss.

Obvious initial targets are the large funds transfer networks, such as SWIFT; domestic banking, and the now common method of access, the Automatic Teller Machine (ATM), is easy to cripple. Also targeted could be the credit system, including credit cards and credit bureaus (TRW, CBI). The average individual in Western Civilization has grown dependent upon plastic and 'vapor' money of the Electronic Age; commonly they have less than $100 (U.S., 1993 dollars) in negotiable tender on their person, trusting in their ability to quickly and conveniently get what they need.

This is all, however, just icing upon the cake. It is possible, with a little help from the systems already in place, to destroy the world's currency, capital, and equity markets in a matter of minutes. As the speed of technology came into play in the financial world, the brokerages and financial organizations quickly took advantage of it; it is now a competitive requirement for massive computing power to be constantly watching all the markets of the world, performing analyses, making decisions, and executing orders entirely without the approval or intervention of a human being. Such systems, called 'program trading,' have trillions of dollars at work directly, not counting the leverage gained from their positions; insertion of the right type of orders into the right machines would be devastating and trigger worldwide panic and financial collapse (for instance, the Japanese brokerages selling all their U.S. dollar positions, bonds, and stocks, coupled with reactionary orders in the American trading systems). It is odd that with all the speculation of disaster regarding the removal of humans from the decision loop for military technology, no one recognized the worse impending danger on the economic side.

2.4 Transportation/Logistics

Western Civilization has become so specialized that it is no longer has self-sustaining population centers; once basic logistics are disturbed, such centers of population are at great risk. Aviation is simple to paralyze; air traffic control systems are essential for any civilian flight. For sheer nuisance value, collateral systems such as the SABRE scheduling system could also be targeted. Shipping, trucking, and rail transport can all be crippled through their scheduling and coordination systems.

[The topic of transportation brings a small digression: an analysis of airport anti-terrorism security measures leads to interesting conclusions. It would be educational for the reader to consider the focus and results of terror attacks involving air travel pre- and post- introduction of airport metal detectors. Security measures seem to only have worsened the situation; how does such a discovery extrapolate to the introduction of thermal neutron analysis devices? TNG principals have analyzed the TNA device and conclude that the next generation of such terrorism will involve unary or binary chemical weapons, or non-nitrogen 'firestorm' type weapons, such as thermite (ignited by magnesium triggered by sodium metal set off by a water pressurization fuse). The more things change, the more they remain the same.]

2.5 SSA

The Social Security Administration is 'the hand that feeds'; it is also an easy target. This system, which provides payments for welfare, social security, and veterans, has no protection, no auditing, and no hope of restoration once removed.

2.6 IRS

The Internal Revenue Service quite recently made it possible to tamper with them. Introduction of 'electronic filing' of income tax has created the opportunity to flood their system with bad information (taking names at random from the telephone rolls, accessing the credit reporting system to gather essential information such as their taxpayer identification number and financial status, and then creating a 'bogus' tax return which would be filed).

The IRS system is one of the few 'hard' systems (meaning it has some of the better electronic protection), but it is targetable in two ways: an EMP generator, generating a damaging static charge of 50K volts to any conducting object, can be used to eliminate the system, or the system can be attacked in the same subtle fashion as the most 'secure' electronic systems in Western Civilization (see the section on 'isolated' systems in the Government section).

2.7 Communications

It could add considerably more terror and panic to incapacitate the conventional means of mass communication, cable and commercial or 'network' television. These system are completely dependent upon electronic switching, microwave, and satellite pathways for their deliveries, and security of such is poor, most attention having been focused at prevention of theft-of-signal.

2.8 Government & DoD/Intel

Oddly enough (for one would assume that this sector would be secure), a crippling amount of damage can be done to the government sector. The group responsible for protecting the West against just this sort of an attack, the National Security Agency, has been sorely remiss in their duty (just one small example: The brain trust in charge of technology security for the U.S. let their classified procurement records through most of the 80s be released in a database (Maryland Procurement Office);

worse yet, they didn't know it until they were told by an outsider. Knowing what they were buying provided a good degree of intelligence to the opposition; it also opens a future hole by exposing the type of technology to target to do them damage.).

Granted, making any technology secure is difficult; just as with a locked room, there are plenty of ways to pick a lock, force a door, steal a key, make the owner let you in, or just go through a window. Add to this that most of the people who are supposed to be protecting things are completely incapable of doing so--like virgins talking about sex, they are beyond their competence. There is, however, a sincere amount of deliberate negligence. Their rationale has been that protecting U.S. technology would be dangerous, as it would be exported or stolen, and then the U.S. would be in a position of being unable to break into their own systems, then in the hands of enemies. The implication, of course, is that NSA takes its job of being able to penetrate target systems as more important than protecting the West from a similar danger. Sheer folly.

NSA systems, such as the old PLATFORM network and their in-house system Dockmaster are difficult, but not unassailable targets. The scientists at NSA are counting on their 'isolated' systems to be impervious to this sort of tampering; it is unfortunate (for them) that there is no such thing as an isolated system. Even if the system is behind a giant 'blast door,' with supposedly no contact to the outside world, with the software written in DoD approved ADA, the system is still 'touchable.' The system has an operating system, other applications, the ADA programming tools and compilers, and a host of other mechanisms exist for getting something 'in' to the system, and that's all it takes. Even if the Defense Department were to institute prophylactic measures to attempt to keep such things from happening, Precipice style attacks can target through contractors and other suppliers, making all systems available for informational warfare attacks.

Precipice poses as serious a threat to the military strength of the NATO forces. It was the acknowledged technical superiority which enabled a quick and painless (for the West) end to the Gulf Conflict. Such an 'edge' can be removed quite simply, evening up things considerably (actually, more than evening up--today's typical NATO soldier is mostly helpless without his technology to back him up). Even the tactical nuclear devices will become unusable, as the 'PAL' codes that activate them are not kept on-site in a 'hard' (printed, for example) format that is readily usable; without such a code, which are individually unique per device, things like atomic mortar rounds equate with throwing rocks.

NATO tools of policy, such as Japan, the U.S. mechanism of choice for Asia, are also at risk. Japan is currently updating and relocating its antiquated equivalent of the 'Pentagon.' Analysis of the proposed new installation leaves Japan in a more vulnerable position that it is currently (which is pitiful; CIA has volubly and accurately complained that Japan 'leaks like a sieve' and has rightly refused to share crucial intelligence for just that reason).

Groups in the intelligence community will be hit even harder. As intel moved from HumInt to SigInt, it became more and more susceptible to 'spoofing' (tampering with the signal) or outright destruction of the means of gathering and analyzing the endless amounts of data generated by such systems. For instance, the CIA uses NeXT workstations, notoriously easy targets, for image analysis; the billions of dollars of satellite surveillance gear circling the globe becomes worthless if the systems aren't there to make sense of it (not to mention the risk to systems such as the ARGUS ring). Precipice style informational warfare attacks make an easy target of all C4I (Command, Control, Communications, Computers, Intelligence).

Law enforcement organizations are a mixed bag of security problems. Police, the Secret Service, and the Justice Department could all suffer greatly from major attacks; introduction of systems such as the Federal Crime Information Center, with fingerprint tracking, etc., if they pass the test of the ACLU, won't pass any security test. These groups have already been subject to a considerable amount of scrutiny by the 'underground' and are already thoroughly penetrated; for example, the Drug Enforcement Administration has been penetrated through their primary contractor, leaking names of informants (now deceased) and details of their system. The only group that has a mixed blessing is the Federal Bureau of Investigation, which still relies on pre-microchip technology and techniques for most of their work, lending them some immunity.

2.9 Business

Attacking the business community of the West is trivial compared with other targets. A simple tactic of hitting with maximum stealth and aiming for maximum damage with 'military grade' worm, virus, and penetration attacks will overwhelm any resistance they can offer. Some small protection against electronic attack has been implemented in the business community, yet it has a set of fatal flaws; such protection systems look for 'known' signatures of attack mechanisms, but the new and novel pass right through. Primary targets will be the mainframes, microcomputers, and networks that businesses in the West rely upon for everything from simple word processing, to decision support or factory automation.

2.10 Exploitable holes

Precipice style attacks can take advantage of the fallout from Western power politics and backstabbing. NATO paranoia prior, during, and subsequent to the Gulf Conflict has made Western leaders nervous about providing advanced weapons systems that may be turned against NATO forces by their current users, or, as was the worry with Saddam Hussein approaching Saudi Arabia, by someone acquiring them.

Because of this, the U.S. wanted the ability to deactivate or destroy, via a coded signal, any weapons system that is of American manufacture via 'software.' Such systems are also deliberately vulnerable to electronic penetration attacks (as per NSA doctrine). In an odd twist of irony, Japan has also likely implemented into their technology of military use the ability to destroy or deactivate the system at the hardware level; this is part of a veiled but very real and operational "Japan That Can Say 'No'" strategy that has shown up on occasion throughout our analyses. Knowledge of this weakness has caused the NSA to initiate its own chip manufacturing efforts for critical systems; this effort was out-of-date and outclassed from its inception.

3.0 Non-conventional warfare

We are witness to a new 'theatre' of operations opening up, where the antagonists can be anywhere, at any time, with immense leverage of their resources all out of proportion to the damage they can cause. The training grounds, a 'virtual' place, are not something that can be tracked by satellites, but more live within them; the entry cost to get in the game is so small as to be negligible, something that can be paid for as a by-product of 'riding the grid.' The profile of those capable of informational attacks is a combination of 'Carlos' and 'Robin Hood.' Today is the tomorrow you worried about yesterday.

3.1 NCBI

The crowning glory of non-conventional warfare are attacks carried out using nuclear devices, chemicals, biological weapons, and, as proposed herein, informational attacks. All of these mechanisms are known for their large, rather indiscriminate capabilities of destruction; informational attacks are additionally 'tactical' and can be quite surgical.

3.2 Informationals

As has been outlined previously, this is the primary method for a small group to leverage themselves into a considerable force; what one doesn't have the numbers to make short work of, one needs to stretch out over time. Technology provides the necessary ability to introduce systems over time and in such numbers as to create quite a stir at the previously appointed time, yet this can be done by a few or lone antagonist, and from anywhere they can hook into the 'grid'.

All that is required is the use of sophisticated electronic penetration techniques, computer worms and viruses, and the exploitation of existing 'targets of opportunity.' Such knowledge does not, as yet, grow on trees; there are perhaps a few handfuls of individuals with the necessary skills and desire to carry out a program such as Precipice.

The viruses and worms needed to execute the project are not terribly complex; indeed, this is a benefit, as such 'weapons' have only been discovered in the past through malfunction or when they had activated, post damage, usually in isolated circumstances--yet a full scale attack such as Precipice would target widely, and leave no room for response. Each specific target could be covered by redundant attacks, with one attack being a stealthy, bare-bones style intrusion (ideally a custom built attack aimed at each specific system, rather than a 'shotgun' approach), with the other being new, previously unheard of technology such as:

Morphing viruses, which constantly change their programming code and configuration to avoid a stable pattern that can be looked for;

Binary attacks/data viruses, which reside, Trojan Horse fashion in legitimate systems as only a few necessary bytes, only activating upon linkage with the remainder of the system which was disguised as unexecutable (and hence, a blind spot for 'hunter-killer' prophylactic systems) data files, or a section 'hidden' in 'unusable' sections of the system; such systems also pass through 'firewall' style protection;

Polymorphic worms, which are slightly cumbersome, but can reconfigure themselves to cross machine type boundaries, thus avoiding a 'yeast growth law' limitation to the spread;

'Factory' worms, that take advantage of networks hanging off of networks, by breaking into the 'parent' system, taking advantage of the newly available trusting resources and accesses, then propagating and seeding throughout the 'child' network(s), mutating, and then launching back through the gateway into the larger network;

Cryptographic worms, which infiltrate into the storage mechanism of the system, and encipher with a public-key system all the stored data, and decipher the retrieved data for a period of time, until one day the retrieval half of the pair 'commits suicide' and performs a low level format on itself, thus making all data in the system non-retrievable; note that this attack is deliberately reversible by the reintroduction of the decryption half of the worm;

Envoys, or expert penetration systems, that use knowledge-based system technology to learn from the penetration team and carry out further penetrations on its own.

The main group intended to 'combat' such infiltration, the National Security Agency, has been covering their inability to correct the problem for many years now. NSA relies upon 'secure' system metaphors such as the MULTICS model, yet these were invalidated years ago by the advance of such penetration technology (which can, in fact, use the protection mechanisms to their own advantage). Quite simply, there is little hope to prevent such intrusions.

4.0 Rationale--Who and Why

How would one benefit by such actions as the Precipice style attacks? Who would it profit? As with most things, there are varying colors and shades. Taking the two extremes and examining them is highly educational:

4.1 Full Scale Attack

Once the triggering event has occurred, John Doe and Jane Roe are in sorry shape. For instance, immediately there is no phone, police access, fire control access, medical care for emergencies, alarms, power, sanitation, money, credit cards, financial markets, economy, social programs, television, government or intelligence community. There will be limited transportation (none on a large scale, no logistics, personal transport is mostly temporary as fuel runs out, leaving muscle power), and supplies (food, water, fuel). Likely there will be military with conventional weaponry, their stockpiles, and radio communications available to them.

What happens next is pure supposition, but some things are clear--there will be immediate chaos. Control will be established after a certain period of time; society has a certain inertia holding it together. In the interim, the amount of damage that will be done will total into the trillions; this does not take into account the long term economic effects which will be uncorrectable.

The West will be suffering near-fatal internal strife, and will be quite unable to cope with anyone else's problems at the time. Even afterwards, if control is successfully reestablished, the countries of the West will be, at best, Second World parties, and unable to exert any real influence beyond their own borders for a time.

In what context is it desirable to destroy Western Civilization, primarily those countries that comprise what is known as NATO (North Atlantic Treaty Organization)? When the executing parties have something to gain--possibly their independence from NATO dominance, influence, and manipulation.

Historically, a 'breaking away' of this sort has only been possible when the dominating country was heavily involved elsewhere, financially strapped, or incapacitated. Even the American Revolution (1776 A.D.) was only possible in the context of Great Britain being quite occupied elsewhere. It is also humorous to note the symbolic 'first act' of that rebellion was economic, the dumping of commodities at the 'Boston Tea Party.'

The rules of rebellion are different than they were for the American conflict; the best model for running a modern effort towards self determination was the World War I effort of T.E. Lawrence and his compatriots. Such lessons come mostly in the form of "don't"s:

Don't attack militarily (it only forces the game to be played by the opponents rules, rather than your own [Iraq's miscalculation in the Gulf Conflict]);

Don't attack your opponent's strength directly but hit around the target (destroying logistics, for instance; increasing terror, or helplessness; not falling into a predictable pattern; obvious targets are commonly the best guarded, pitting your forces against your opponent's strength, a serious mistake);

Don't lose or give up your mobility, your foe isn't going anywhere (and if they do, it means you've won, incurring a whole new set of problems);

Don't let your opponent fight a single- or double-fronted war, always force them to maintain a hyperextended (thus overextended) front;

Don't fight a pitched battle, even by mistake, always maintain 'hit and run' tactics that give your forces the advantage;

Don't strike indiscriminately, or strike just to strike, be surgical in the precision with which operations are carried out;

Don't pick simple targets; seek leverage, go for 'more bang for your buck' style targets that cause extreme damage for little effort.

Western Civilization is wide open to attacks governed by these rules--it certainly isn't going anywhere (no one is packing up New York or Tokyo and moving them), mobility and time are on the side of the attacker. In fact, the best method of making such an attack by such 'rules' is by hitting the infrastructure and economy of the NATO countries and their dependents.

A few parties have the greatest desire to see this done; for instance, the Middle East has been the battle field since WWI, and post-WWII, because of the importance of oil and the West's need to control it. The Cold War raged through the region, with the U.S. using Israel (and later Egypt) as a tool of policy and control, ignoring even the most blatant human rights violations perpetrated by the Israelis and other allies against the Palestinians and other targets. But, similar to the way the Spanish Empire ran afoul of the harmless people they drove into the seas, known as the Buccans (for the fires over which they roasted the pigs the Spanish had seeded the islands with) and later as pirates, the Arabs refused to take the situation lightly and have been fighting ever since. Another interested and injured party would be in Ireland; long the target of British oppression, up to and including the earliest programs of organized, State-sanctioned genocide, certain among the Irish have desired self determination for centuries. A 'bytes, not bombs' strategy could be quite appealing to guerrilla and terrorist organizations world-wide; this comes from an increased awareness of the 'feedback' loop that terrorism makes possible. While it has been desirable (from their point of view) for such groups to attempt to force a government response to restrict civil and (in some cases) human rights to foster a feeling of oppression in the general populous, it usually only increases the militarization of anti-terror forces while not appreciably inconveniencing 'the masses' and can cost popular support. A shift in focus to terror activities that are not overtly violent would take away much of the justification of government forces for heavy militarization, would cause more damage to the system than their current methods, are safer for the terrorist, and the only option of response by government forces would be 'regulation' of technology and the jeopardized industries (which is a non-viable option).

The wish to have 'Uncle Sam' and his allies out of their lives have driven many a people to wage an up-until-now fruitless war. Something like Precipice would give them a new option that would break them free. Luckily for the West, the emphasis on the part of such parties has remained 'conventional' militarily, with some focus for their intelligence (including the education of their people in the West) on nuclear power.

The Western intelligence community has been in a difficult position regarding the Middle East (Arabic and Islamic) terrorists. One of the 'rules of the game' is that mutual deterrence works, or at least it used to. The U.S. has long had the ability to track the perpetrators of terrorists acts, knows the training base locations, etc. What has held back reprisals? Other than the obvious "don't blow your source" issue, there has also been a sort of "gentleman's agreement"--the U.S. wouldn't hit them, and the U.S. itself was immune from attacks on 'home territory.' The new players aren't following the rules. What makes something like Precipice attractive to players in the Middle East is two-fold:

It strikes at the very heart of the 'Great Satan';

They don't pay nearly as high a price as the West; other than the very top of the society, there is little intrusion of the benefits of the West, and even then, the pro-West aristocracy is hit, not the ruling elite of Islam, for example. A return to the simplicity of the 14th Century is attractive to these people.

4.2 Limited Conflict

Rather than all out 'nuclear war,' a small 'tactical' war is more likely, and more insidious. The two initial segments motivated to play this sort of game are dissident factions in the West and economically motivated concerns.

There are numerous internal elements of dissension in the West who would see this sort of an option as useful for its real or 'threat' value; the power to destroy something is the power to control it, and there are 'oh so many' ways to cause trouble.

Informational warfare attacks could be racially motivated (the neo-Nazi movement is quite motivated in the technical arena), terrorist launched, started by eco-terrorists, part of a blackmail attempt, or just a casual action by hostile parties.

Money is also a great motivator; a new degree of low-level conflict could mean an economic war of sabotage by 'allies' against each other (witness the programs initiated in Israel and Germany to build a competence in Precipice style attacks), or American usage against hostile 'economic' targets (not outside the realm of possibility; view it as the next step after sanctions--"If you won't stop selling X to Y, then we'll make certain you can't make X."). The Japanese are also gaining an understanding of the techniques and strategies as a side effect of their broad-based competitive intelligence programs. Additionally, industrial spying is breeding a subculture geared for this sort of work; the electronic criminals (hackers, crackers, and cyberpunks) discovered that 'stealing' money led to their being caught (the old game of 'follow the money'--you have to pick it somehow, somewhere, some day), while stealing information was much more lucrative and virtually untraceable.

The 'Information Age' is more like the 'Wild West' than anything else--there are no 'rules' to break, so it is a 'land' of opportunity. Targets in the West are too susceptible, not just to destruction, but to disruption, spoofing, and passive spying; all systems that technology touches in the West can be considered compromised.

5.0 Conclusions

How to conclude? The problems are there and aren't abating; I can draw conclusions, but there are few solutions. The buzz about information warfare will begin to occur as more and more people become technology savvy; just as with the initial reports of computer viruses and worms, I expect people to slap their forehead and say "I can do that!" By any account, I'm certain they can, and will.

[This article was originally written two years ago. Oddly enough, at the time nobody knew what I was talking about; since then, the topic has been mentioned in The Economist, The Wall Street Journal, and a wide variety of very poor books. I feel even more strongly today than I did then--it is just a matter of time. What I didn't expect was that the capabilities necessary to wage this sortof war would crop up in more than myself and a small group of people I'm familiar with; so much for being egotistical. As the old Chinese proverb goes, *'May you live in interesting times.'*]

Ω

Jim Teff's Magic Elixir

This is a great energy drink, thirst quencher, and general tonic.

For one glass, take approximately. 8 oz. of water and add one tablespoon of apple cider vinegar and one tablespoon boney (adjust to taste). For a 32 Oz. bottle, use 1/3 cup apple cider vinegar,1/3 cup honey, and fill container with water.

Poor Man's Bota Canteen

This is priced right and holds more liquid than bike bottle. Take one 32 Oz. dishwashing liquid squirt bottle, rinse throughly with hot water several times, then fill with vinegar and let sit for few days to kill soap taste. A carrying strap can be made by taking a piece of paracord, leather thong, shoelace, or similar item tying it around the neck, and making a carrying strap loop with the free end.

Ω

Letters

We'd like to hear from you. Your suggestions, comments, commentary, opinions, feedback, and what-not is always welcome. Send it to:
Cybertek
P.O. Box 64
Brewster, NY 10509
ATTN: Feedback

Dear Thomas:

For years I dreamed of one day walking off, leaving society and living in the forest hiking from towns to camps of disenfranchised Hippies farming and squatting in the forest.

Most of my assets were purchased with the concept of use under a self-reliant campstyle life - with very little interpersonal interactions outside of the romance of inter-commune travel.

This was after the System's failure of course, and this dream was long before satellites and infrared scopes.

I must learn to use the technology of my parasitic foe - ever hungry law makers, because as we saw in Chechnya, the battle no longer belongs to the brave or strong, one must be cunning as well.

Thanks. - J.P.

Welcome to the Blue Oak Republic
founded 25 March 1994 by
Millennium Twain
Post Office Box E
Menlo Park, CA
94026, USA

The Blue Oak Republic is not a territory, nor a government, nor an organization:

It is the recognition of the limitless freedom of individual character and achievement, by an individual.

It is the identification of _infinite_ individual natural and expressed rights of private thought, communication, experience, activity, exploration, creativity, productivity, contract, ownership and enterprise.

It is full acceptance of the private responsibility for ethical integrity -- towards self, family, company, community, and nature.

To make the Blue Oak Republic a reality, just affirm the following Constitution or First Principles:

No harm or coercion will ever be directed by me against any other person or persons, against the property of others, or against nature.

I will always defend against wrongful violence to myself or others or the environment, utilizing all the power within me.

I will never construe the healthy individuality of perosnal character, or the creative activities of community, or the natural growth of industry and economy (in harmony with nature) as violent in any way.

Signed _____

[Please copy, post and distribute]

Ω

Classifieds

Hacking / Phreaking / Cracking / Electronics Information / Viruses / Anarchy / Internet information now available by computer disks, books, manuals or membership. Send $1 for catalog to: **SotMESC, Box 573, Long Beach, MS 39560**

UNDERGROUND INFORMATION: Computer Security, Hacking, Phones, Survivalism, Cryptography, and more. Catalog **$2. SHP, 862 Farmington Avenue, Suite 306, Bristol, CT 06010**

CONSULTING SERVICES AVAILABLE: Information and Electronic Security, Disaster Preparedness, Personal Security/Self-Reliance, and Specialized Communications Systems for individuals and businesses. **Reasonable rates** as

compared to others in the industry with less practal experience in these fields. **OCL/Magnitude Consulting Services, 203-225-1625.**

WANTED: Articles for Cybertek #13. We are seeking high-quality, practical, how-to articles on technology, security, and self-reliance. Unsolicited manuscripts welcome. Write, call 203-225-1625 or email to ticom@connix.com for topics of interest, writers' guidelines, and compensation information, or to submit an article.

Classified Ad Fee: 5 cents/word. 20 word minimmum
Deadline for September/October '95 Issue: August 20, 1995
Send ads to: Cybertek, P.O. Box 64, brewster, NY 10509 ATTN: Classifieds

Ω

Masthead

Publisher
Thomas Filecco
OCL/Magnitude
P.O. Box 64, Brewster, NY 10509
(203)-225-1OCL (1625)

Senior Editor
Thomas Icom
ticom@l0pht.com

Associate Editor
Administrative Operations
Carol J. Filecco

BBS SYSOPS
Mercenary/IIRG
mercenary@iirg.com
Brian Oblivion/L0pht Heavy Industries
oblivion@l0pht.com

Writers
Atreides, Nick Halflinger, Wildflower, Bleach, S.V.M., Jim Teff, Charlie Holmes

Subscription Information
Individual: $15/year (published bimonthly)
Corporate: $80/year
Canadian: US $25/year
Overseas: US $30/year

Trades of similar periodicals, interesting (and functional) electronic equipment, office supplies, envelopes, and 32 or 55 cent stamps accepted in lieu of monetary payment.

"Is is error alone which needs the support of government. truth can stand by itself."

- Thomas Jefferson