Beyond Information Warfare:
The History of The Future of Hacking
(2011-2035)

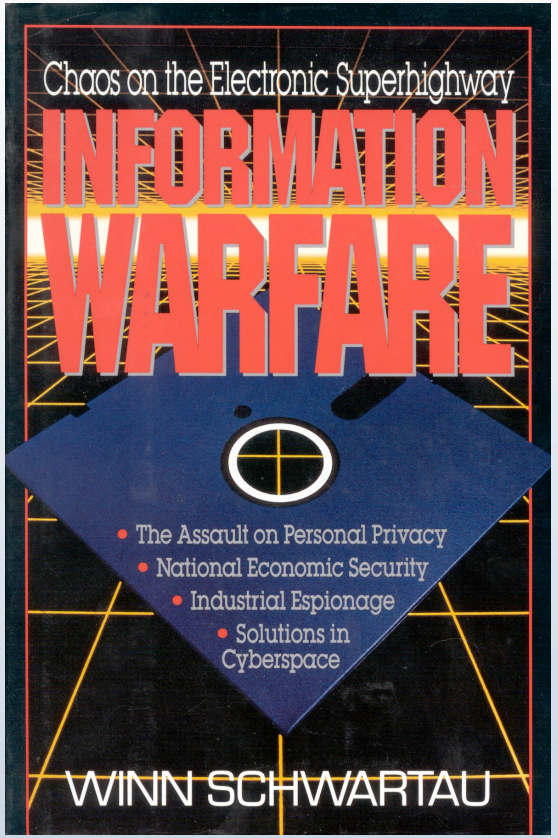
Winn Schwartau,

www.WinnSchwartau.Com

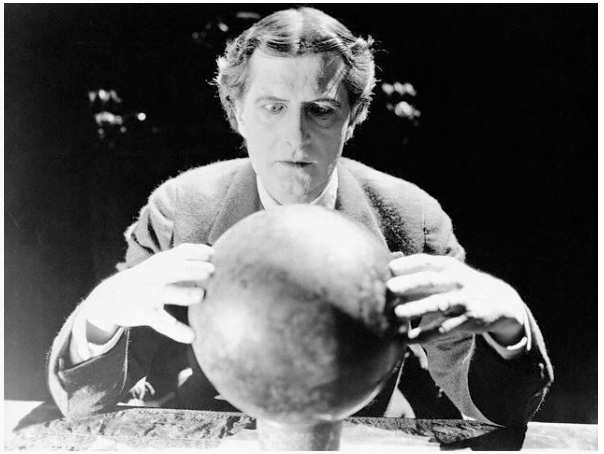
www.MobileActiveDefense.Com

Je ne suis pas fou!

- "Electronic Pearl Harbor"
  - *Winn Schwartau: U.S. Congress June 27, 1991 (Coined the phrase)*
- "Electronic Pearl Harbor"
  - *CIA Director John Deutch Congress,*
  - *June 26, 1996*
- *2011: Everyone says the same*



1989-1994, I predicted:



- The weaponization of the Internet
- Massive Global Organized On-Line Crime
- Identity Theft affecting 100's of millions of people annually.
- The Loss of Privacy
- Trillions of dollars lost every year
- Nation-state cyber-attacks against other nation-states. Chine, Iran etc.
- Cyberterrorism using 'Western' technologies.
- Classified technologies leak: become weapons in the hands of terrorists and criminals.
- And more and more…

We're Still Doing It Wrong:

1984 - Present

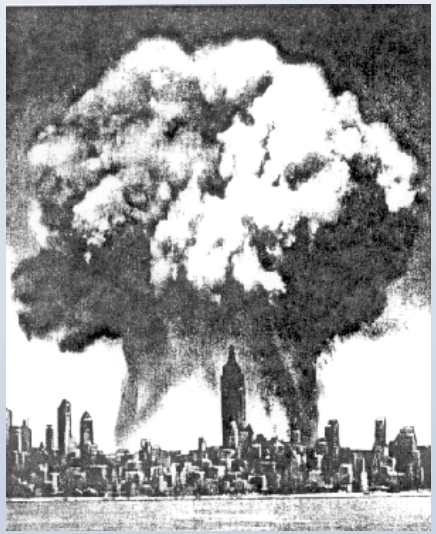
- We, the Information Warriors, have the obligation and duty to do a LOT better job than we have been doing.
- There were plenty of warnings.
  - 1988+
  - Criminals, Extremists and Terrorists.
  - They listened. We didn't.
  - Loss of Privacy.
- We missed our shot with Information Security and it's only going to get worse.

Defenses: We're Still Doing It Wrong: 1984 - Present

- Fortress Mentality
- Brick and Mortar Concepts
  - Defensive IT Technologies
- Perimeter Defense
  - Firewall Perimeter
- Yet we continue to try Fortress Mentality, which we KNOW, historically, will NEVER work.
- What Will Work?

Let's Get Historically Asymmetric

- "Make noise in the East and attack in the West"
  - Sun Tzu ~220BCE
- Mustard Gas
  - WWI - Germany
- Atom Bomb
  - WWII - US



More Asymmetry

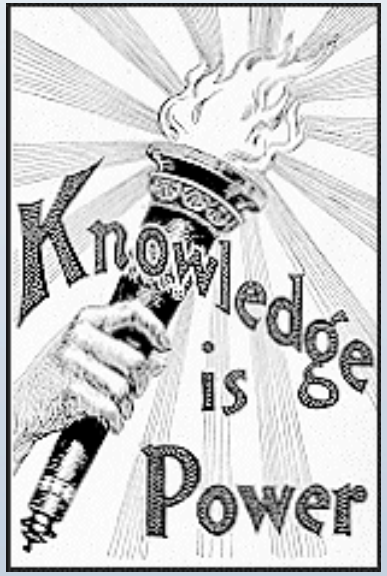
- Unipolar World
  - US sole Military Superpower
- Unrestricted War
  - PRC, Sept. 1998
- 9/11
  - NGO/Terrorists

Three Key Components For Bad Guys To Win Info-War and Beyond

1. Capability
2. Intent
3. Will

Capability

- Access to the technology
  - (That we developed)
- Resources to pay for or develop technology
- Knowledge for applying technology
- Ability to hide/disguise operational readiness
- Private communications
- Shorten time. Expand distance.
  - Force Projection (criminal or…?)



Open Source Technologies can be our Achilles Heel

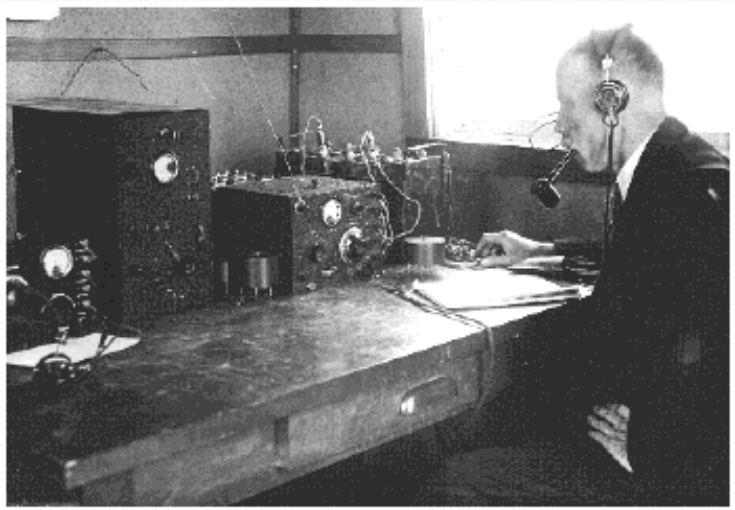
- Equalize capabilities in non-kinetic conflict
- Reduce time of technological lead in new systems capabilities
- "Other Guys" can develop with less bureaucracy or cost

Some 'New' Technologies

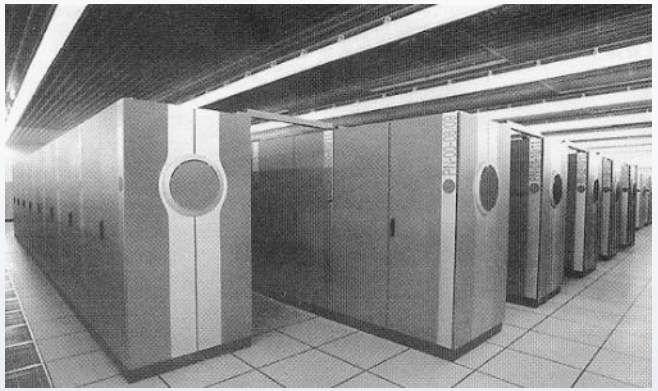
- Bronze
  - Replacing by Iron ~ 1500BCE
- Kinetic Projectile Weapons (Guns)
  - Western US Expansion
- Gatling Gun ~ 1860CE
  - US Civil War
- Aircraft
  - WWI

Some 'New' Technologies

- Radio Communications
  - ~1905CE
- Radar Detection
  - ~1939CE
- Atomic Weapons
  - ~1950CE



The 'New' Technologies



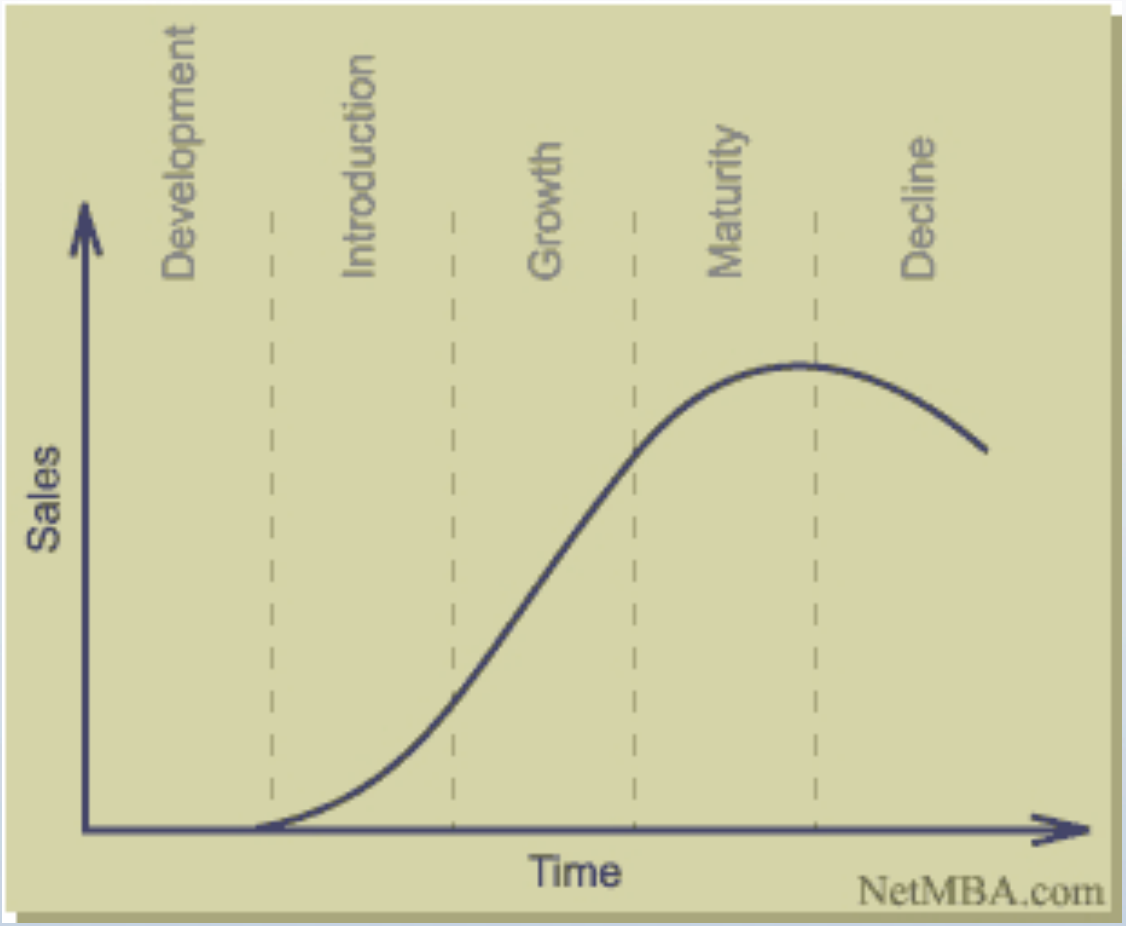
- Super Computers (Dual Use)
  - ~1985CE
  - China is winning!
- Computer Communication (IP)
  - ~1995CE
- Cryptography
  - ~1976CE

Technologies In Development

- All New Technologies Will Be Weaponized
- They always have been, and always will be.

Life Cycle Curve

- Technology
  - Idea
  - Test/Lab
  - Commercial
  - Consumerize
  - Adapt Malware
  - Hostile
  - Weapons



IT Weaponization and Exploitation

- .COM (early)
- .EXE (viruses)
- .JS (hostile code)
- Internal App Code
- The Cloud
- CVE (for all)
- VM
- Wireless
- 3G/4G/GSM etc.

- IPv4/IPv6
- VoIP
- VoMIT
- Spim/Spit
- Html, xml
- XSS
- Crypto
- Steganography
- Chipping

Chat Bots

- Customer Service, Technical Support, Education, Adult online services.

- Chatter
  - Terrorists/Criminals
  - Filtering
  - Adding Chaff

The Source for Artificial Intelligence Chat Bots

The Telephone

- 1920

- Cell Phones:1990

- Today

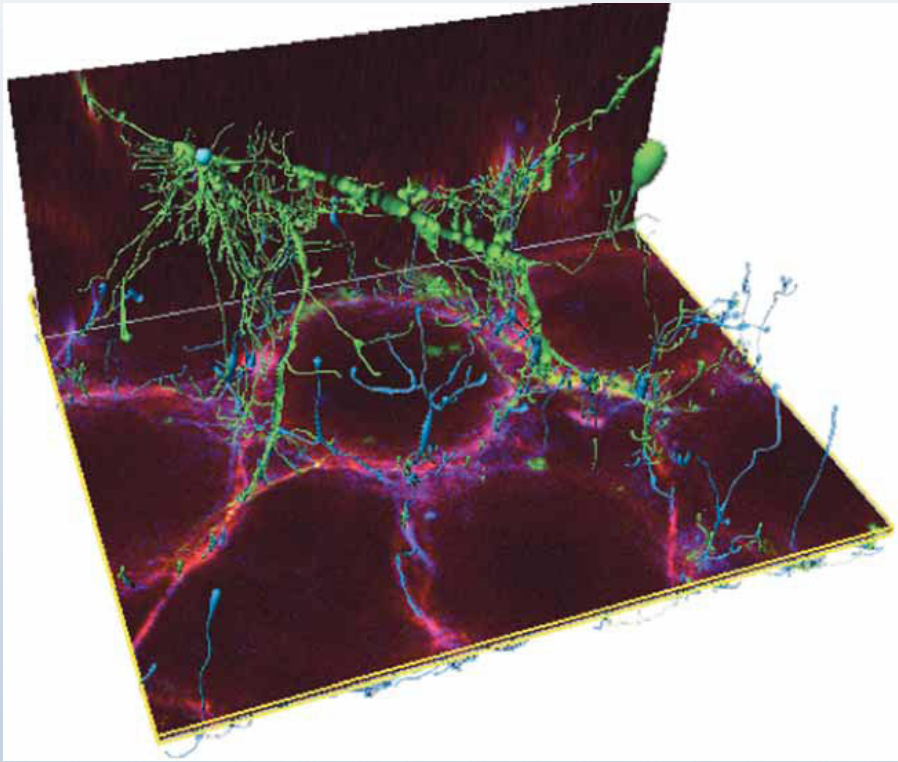
- Tomorrow

Pocket Computers

- 600,000,000 Today
- 2B 2013-4
- 20B 2020

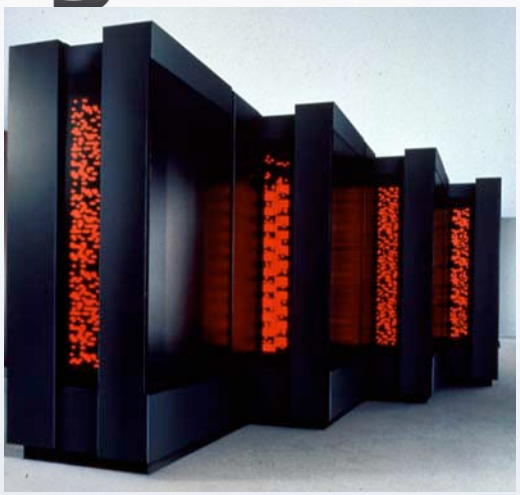
Power To The PC

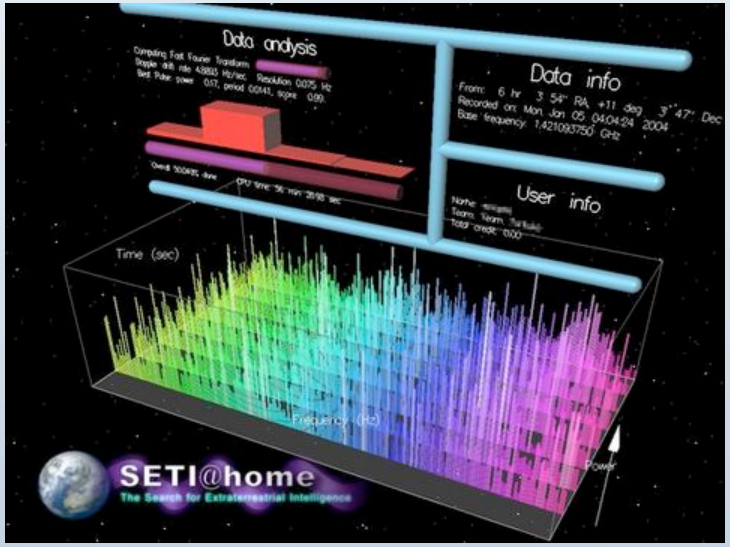
- Room Sized Supercomputer (1980s) in a PC (2009)
- 2029, same power in a single cell
- 2035 = Singularity
- Power to the People?



Distributed Intelligence

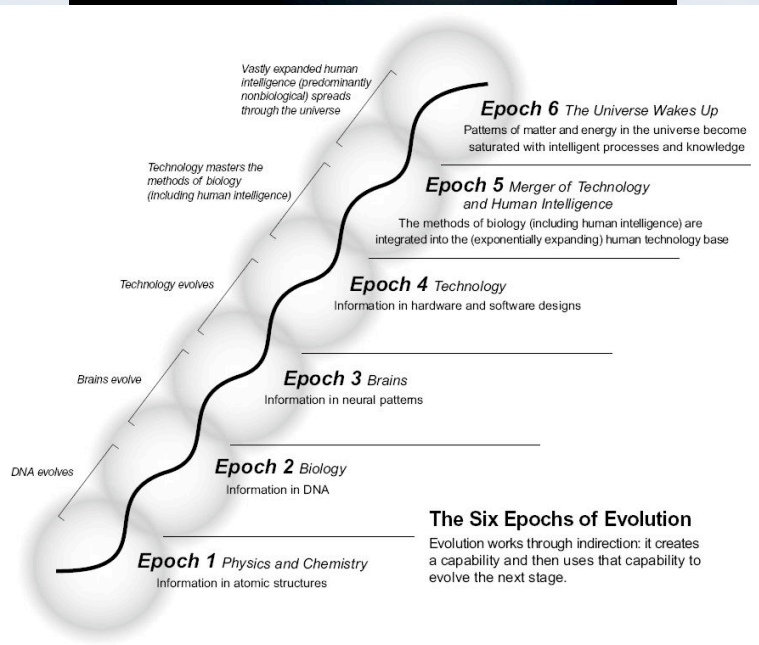
- No need to acquire super computers any longer!
- Use MPP across the Internet a la SETI
- EC2
- Data Mining technology to be used against us!





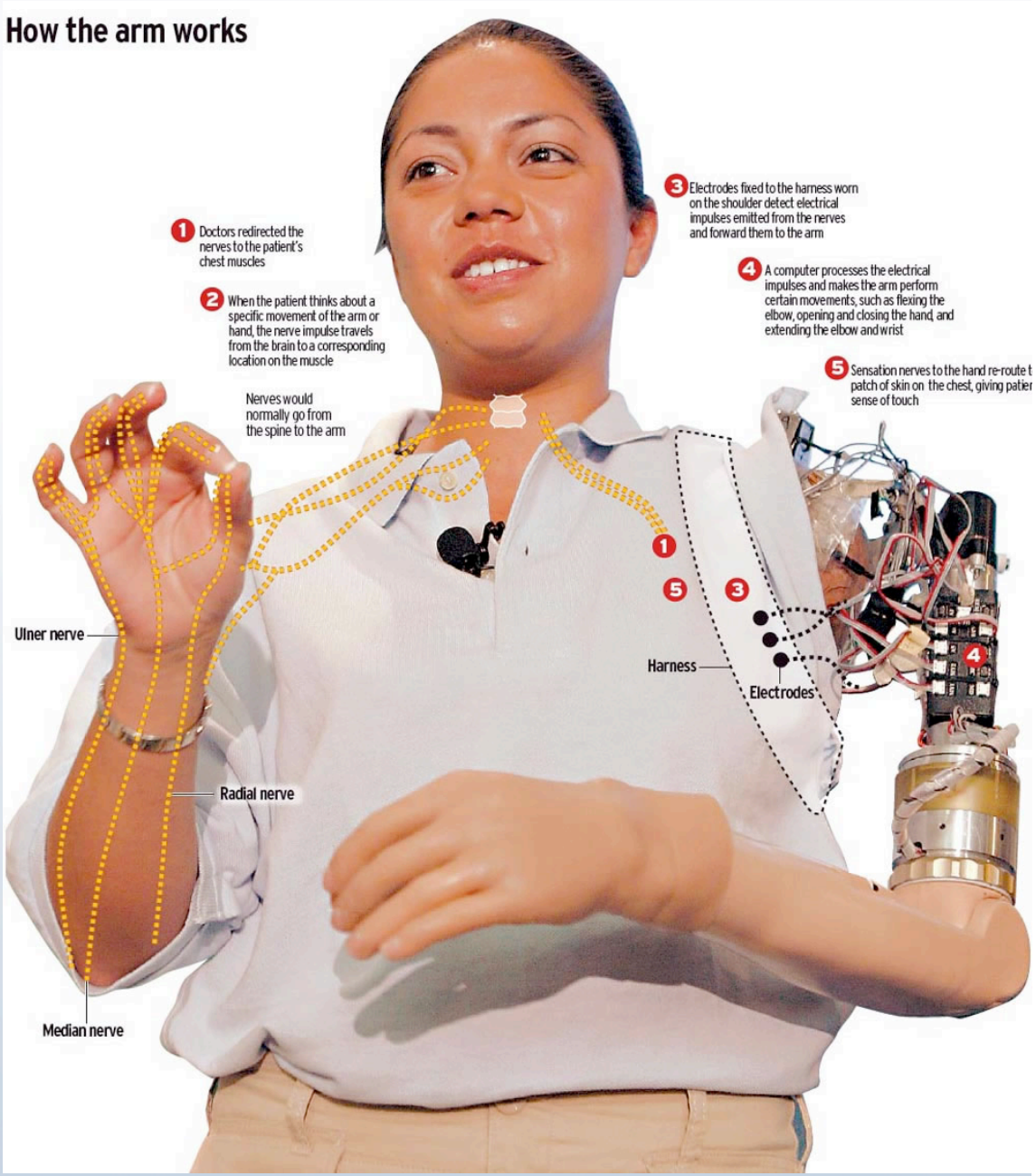
The Singularity

- 2035:
  - The Rise of the Machines (Terminator) SkyLab
- Secure Intelligence?
- Who's Making the Decisions?
  - Machine? Man?
  - Interface (Borg-like?)



Bio-Engineering

- RF Prosthetics



Brain Engineering

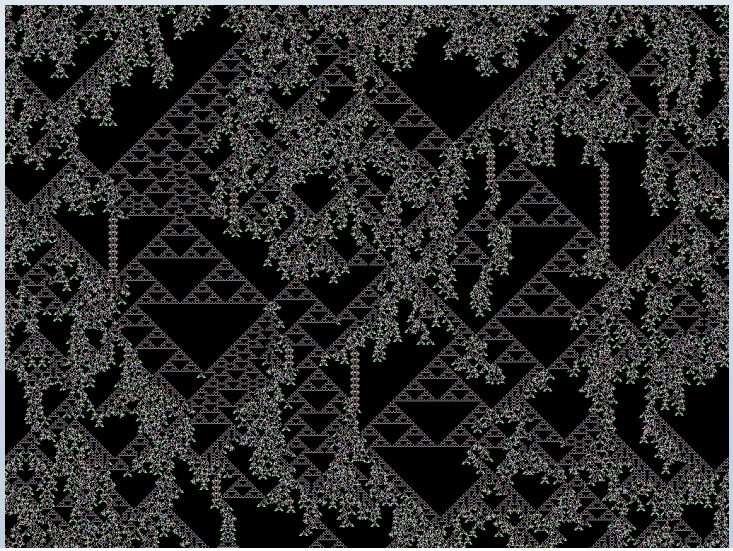
- Brain Control
  - Technology Control
- Mental Illness
  - (electronic Prozac)

Nano Tech

- Can do immense good… or harm
- Nano-toys are on the Shelves.

Swarming & Self Organization

- Unpredictable Outcome
- Simple Rules > Complex Output
  - Automaton, von Neumann (1940)
- Nanogames - Toys R Us

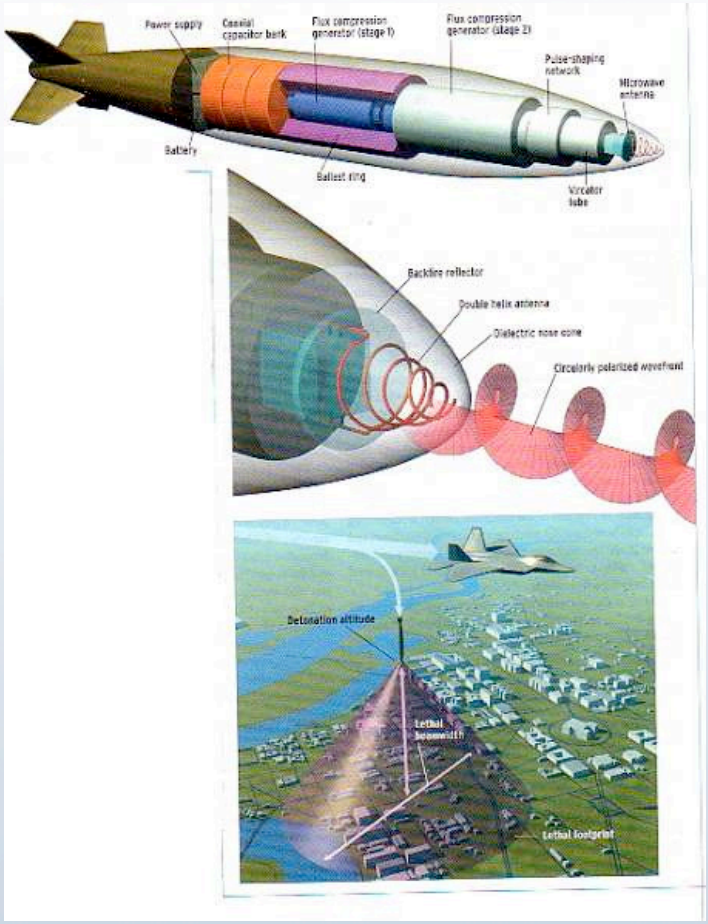


Instigating Chaos

- Financial Markets, Communications, CI
- Public Trust
- Unpredictable behavior of simple rule systems placed in larger 'habitat'.

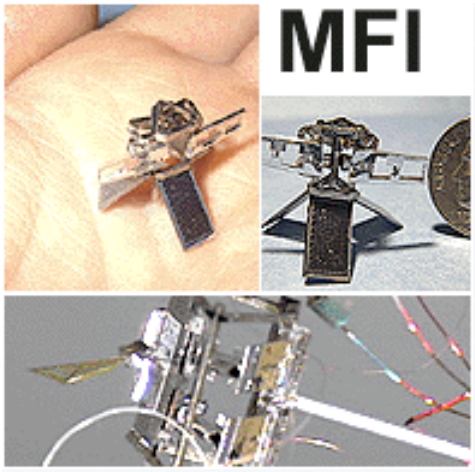
Home Brew HERF & EMP

- 150 Meter range
  - $20 weapons
- 1km Range
  - $500 weapons
- Finance and CIP Targets

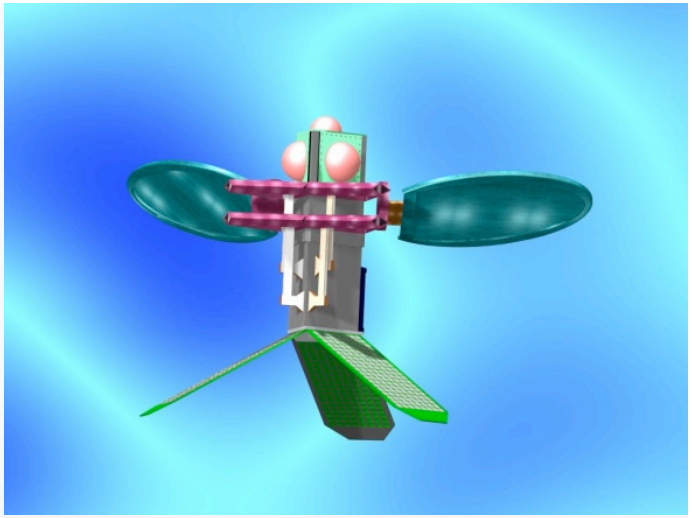


Un-Manned Vehicles (UAV)

- Car Bombs
- Aircraft
- Helicopters
- The Technology
  - Real Time Radio Control/Servo Control
  - Real Time Video in Low Light
  - (Sounds like a kid's toy)



Flying Bots



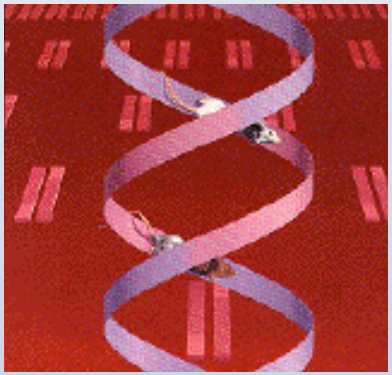
- Technology recently discovered on how to mechanically reproduce birds and flying bugs with new aerodynamic principles.
- Miniature surveillance by flies, ants or other silicon-based "life forms"
  - Chaos
- Nearly invisible Bio-Chem distribution by bots.

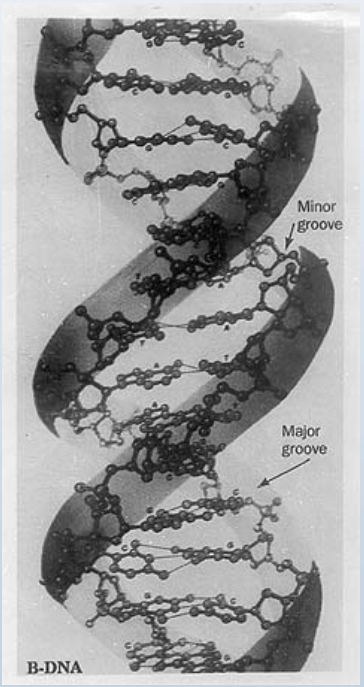
Home Brew Bio-Chem Labs

- Companies sell anything to anyone.
- Open Source information
- Experts in the Bio-Chem field for **$$$**
- 12-Monkeys

Recombinant DNA

- Mess with the ecosystem
- Resilient offensive and malicious microbes





What Can Hackers Do?

- Stop Development (right)
- Build Security In
  - PCs, OS's, Applications, Protocols
  - Plan for the Worst
- Build offensive capability before Bad Guys
- Then notch up defensive posture

Community Solutions?

- International Awareness
  - Conventions and agreements
  - No-proliferation treaties
  - Export controls
- Laws
  - Non-ownership
  - Define legitimate use versus renegade use?
- US/EU
  - Eminent Domain
  - Redefine Threat to US/Free World

One Extreme . . .

- Turn West into a Trusted, Benevolent police-state.
  - No one is trusted.
  - Verify everything and everyone
  - Everything is suspect.
- Xenophobic.
- Monitoring (a la IDS)
  - Behavior
  - Words
  - Communications
  - Affiliations?

Next For Hackers & Infowar?

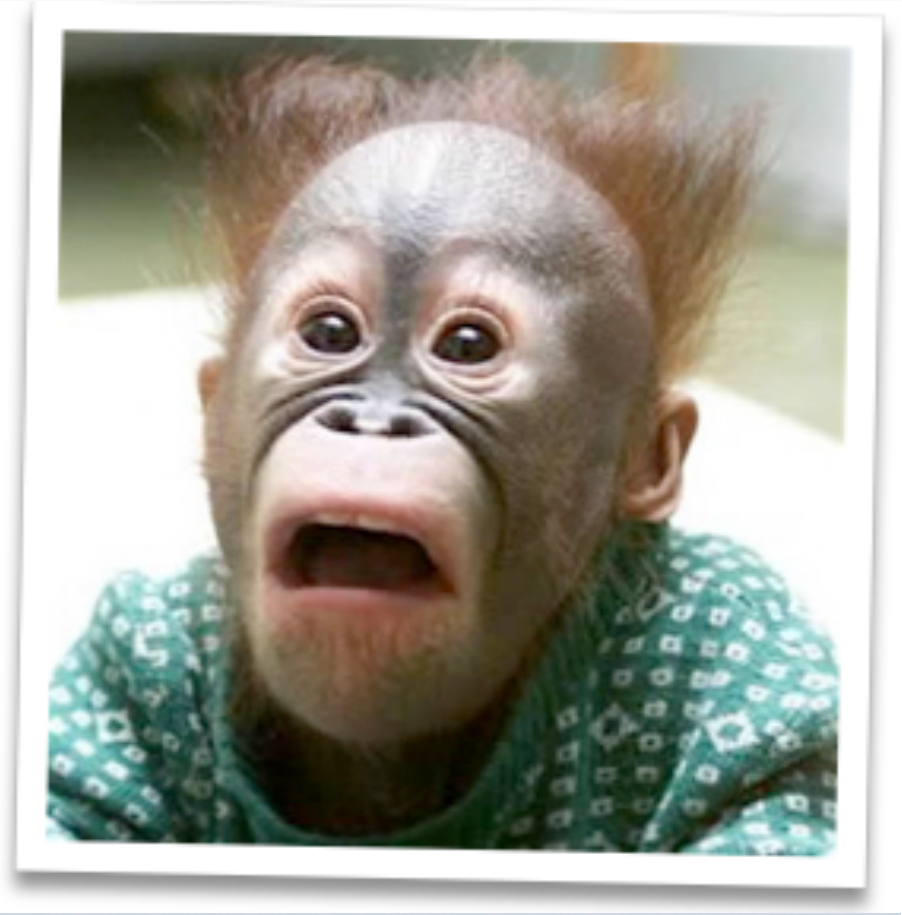
- Realize that we will be 10-20 years behind the bad guys because we are doctrine-bound nationally.
- We started responding to Infowar, CIP and CyberTerrorism after 10 years of warnings.
- CyberTerrorism is only the first step of Tech-War.
- Sitting idly by is a recipe for disaster.

What Scares Me?

- Insiders
  - Access to all/From other 'countries'
  - Different allegiences
  - "Profiling" is necessary
- U.S. + Governments
  - Cyberwar > Bombs!
  - Big Brother
- More "Lulzsec" !

I am Scared Of…

- Vigilantism
  - National
    - Strike Back – Legal or no?
  - How to defend best
  - Attribution
  - Graceful Degradation
- People
  - They are idiots
  - We give them technology

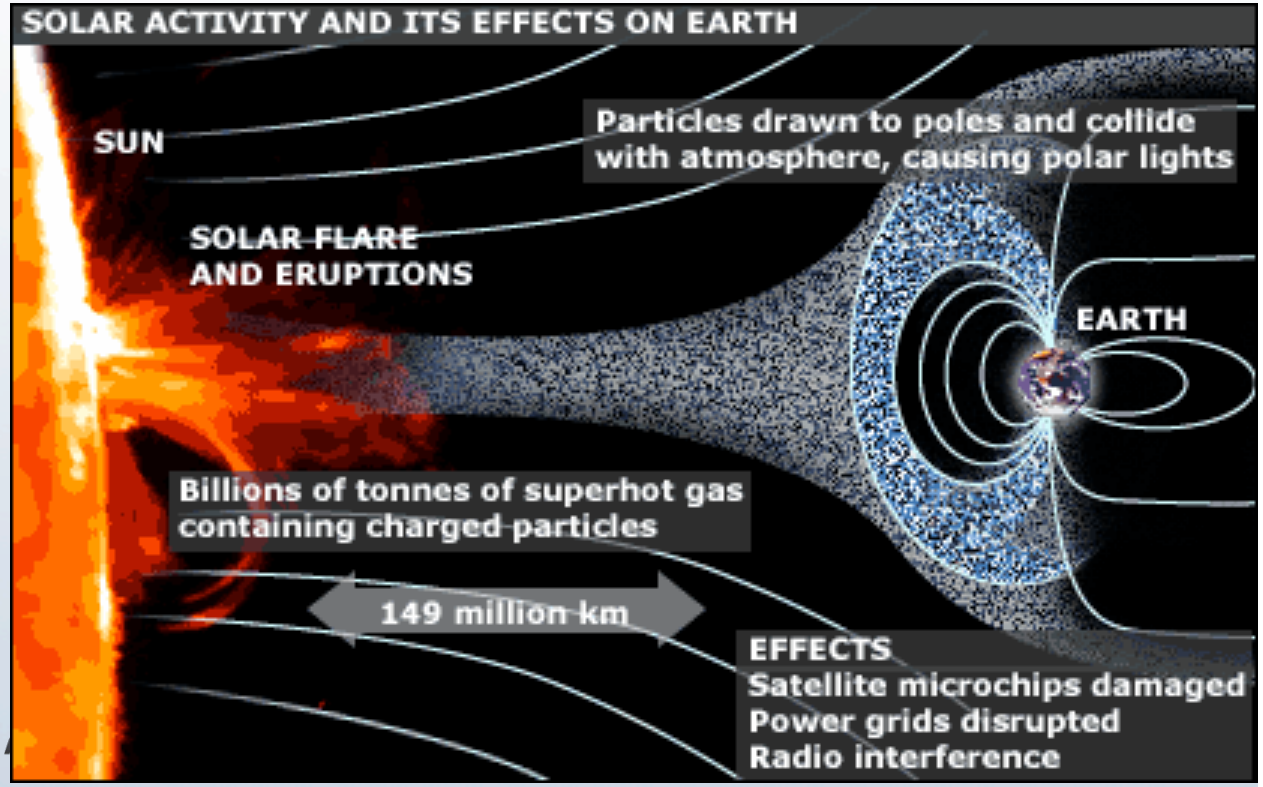


SCARED SHITLESS

at least the horse didn't have underwear to ruin.

Je me chie dessus:

- The Sun: 2012-13
- 1859 – Carrington Event
- Complete Failure
  - Satellites
  - Power Grid
  - Comm
  - Medical
  - Transportation (food, necessities)



Winn's Answer

- Hackers need to develop both offense and defense of all new technologies before they come to market.
- Hackers need to show know how to 'Turn It Off' to make systems more survivable
  - Minimum Mission Critical/Operational Status
- It's our community responsibility!
  - Not the users.
- Ethics, Morals and Social Responsibility
  - Build it right
  - Teach, teach, teach


Questions?
Winn Schwartau
+1.727.393.6600
TheSecurityAwarenessCompany.Com
WinnSchwartau.Com
MobileActiveDefense.Com