CyberWar: Reality or Hype?

Marcus J. Ranum
<mjr@trusecure.com>
Senior Scientist, TruSecure Corp.

Intelligent Risk Management

Overview

- I think it’s all hype
- … now, let me explain why

Some History

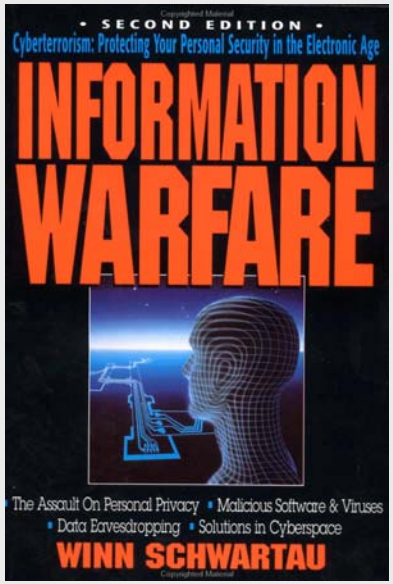
- End of The Cold War, 1992/3
  - Intelligence agencies are worried about funding/budget cuts (“the Peace Dividend”) (which we never saw)
  - Formal computer security was on the ropes:
    - Clipper was a disaster
    - The rainbow series was a failure
  - The Soviet Union’s secrets were all for sale
    - No need to mount an expensive operation to learn about a Soviet tank’s capabilities: buy one on the open market for cash
- The fear-mongers needed a new enemy

Some History *(cont)*

- Winn Schwartau “Information Warfare”
  - Winn’s a merry rogue

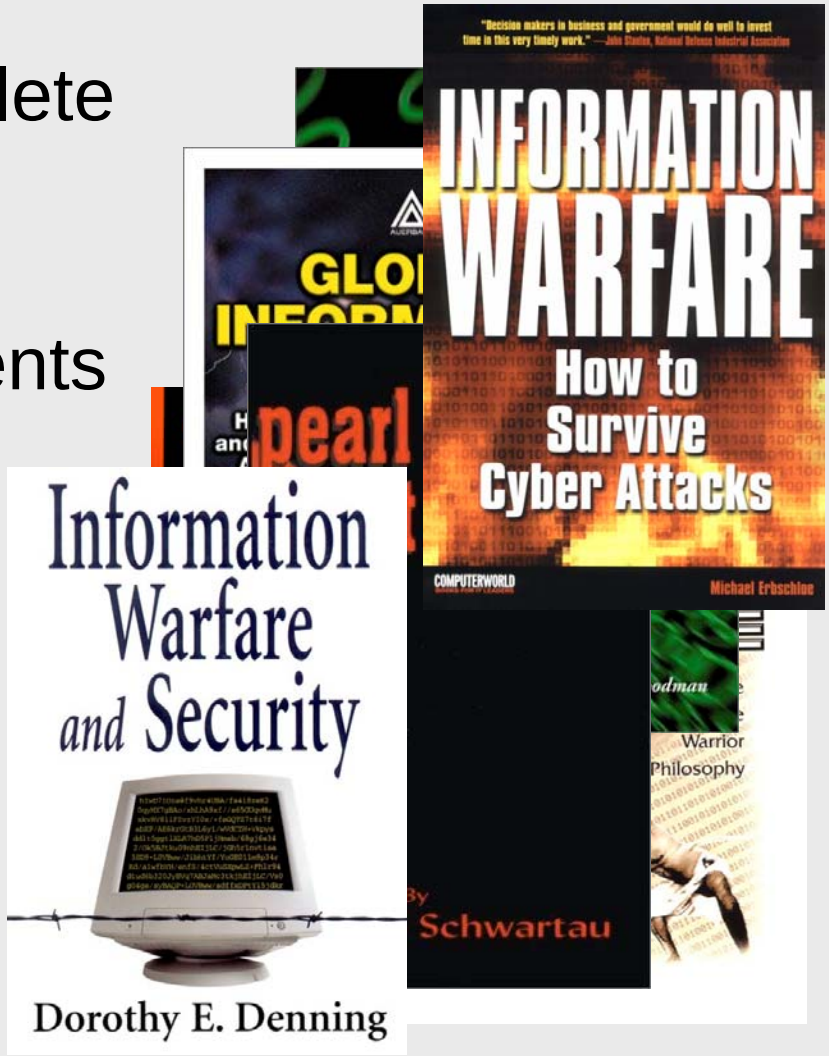
    ...with no background in security (ex rock-music promoter?)
    - First book was a novel about computer security pub. 1991 “*Terminal Compromise*”
  - Book published in 1994
    - Mass of unsubstantiated claims
    - Coined the phrase “digital pearl harbor”

    …and hit a nerve



Some History *(cont)*

- The result was a complete storm of books on "information warfare" without any (yet) incidents of information warfare to justify them…
  - Including from lots of senior security writers jumping on the bandwagon...



Some History *(cont*

- At present, on Amazon.com, there are over 350 titles of books that have something to do with “Information Warfare”
  - “Cyberwar” scores 140 titles

Unclear On the Concept

- The 7 myths of CyberWar
  - Force multiplication (attack synergy)
  - Cost Effectiveness (a weapon for the weak)
  - Economic Collapse (loss of confidence: anarchy)
  - Logistics (keeping weapons to date)
  - In-band attacks (using a network to attack itself)
  - System Administration (compatibility of attacks)
  - Traceability (anonymity in warfare)

Force Multiplication

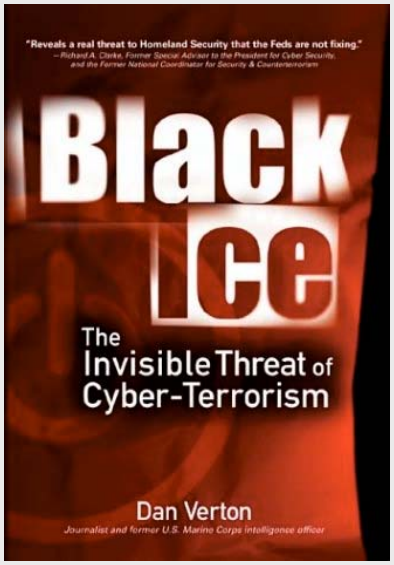
- Premise: CyberWarfare is a force-multiplier that can dramatically increase the deadlines of conventional attacks
- Reality:
  - Most of the examples given are of the variety of layering annoyance on top of a disaster
  - I.e.: your nuclear reactor has just been blown up with conventional weapons; CyberWarriors hamper your ability to coordinate response by disrupting communications

    So what?

Farce Multiplication *(cont)*

- Dan Verton's "Black Ice (the invisible threat of cyberterrorism)" starts off with a breathless scenario of combined CyberTerror attack coupled with physical attack to destroy power stations using hijacked fuel trucks
  - Well, it's *fiction* but someone who can stand up sleeper cells and covert ops doesn't *need* to mess with computers: blow the power and *the computers stop working*

    What ***really*** hurts?



TruSecure® Intelligent Risk Management

Economic Collapse

- Premise: CyberWarfare could be used to destabilize a target's economy (e.g.: shut down all the ATMs or crash the stock exchange) and cause the target to fall into chaos
- Reality:
  - We ***have*** had massive ATM disruptions, power grid failures, or railway system snafus

  We're still waiting for the chaos!!!

Cost Effectiveness

- Premise: CyberWarfare might allow an underfunded (or terrorist) nation to successfully attack a much higher-tech target and do disproportionate damage
- Reality:
  - This might work in the short term but is fundamentally self-defeating
  - It didn't work very well for the Taliban!!
  - Any sufficiently effective attack to "get on the radar screen" invites disproportionate retaliation

Cost Effectiveness *(cont)*

- Low-level attacks such as suicide bombings are much more cost-effective
  - It's easier to convince an ignorant true believer to strap explosives to his body and detonate them than it is to stand up a CyberWar division (we'll get to that when we talk about logistics)

Logistics

- Premise: Actually, the CyberWarfare proponents never ***talk*** about the logistics of CyberWar - ***why?***
- Reality:
  - Maintaining a “CyberArsenal” is not easy
    - Version incompatibility
    - Hackers/grey hats might “out” one of your weapons the day before an attack
    - Target organizations have different security policies and different tools, etc.

Logistics *(cont)*

- Case Study:
  - What would you need, to take the FBI off the air?
    - Something to penetrate one of several kinds of firewall
    - Something to penetrate 2 versions of Windows and 3 different flavors of UNIX servers
      - That can also bypass the A/V software on some desktops
    - Something that would allow you to remotely take control of Cisco routers and switches

      … and it all has to work ***perfectly*** the first time and you can't build a test-bed to develop against

Logistics *(cont)*

- More Likely Case Study:
  - Get a few of the faithful to join the FBI and fire a bunch of claymore mines in the NOCs at a predetermined time

Logistics *(cont)*

- A thought:
  - Outfitting a CyberWar weapons research lab might require: *(secrecy not included)*
    - 10 full-time engineers
    - Managers
    - A switched fabric network + routers + hubs
    - A few varieties of firewalls
    - A few dozen desktops
    - A few dozen servers (of various types)
  - Roughly a $10million/year expenditure
    - Plus, what does the operational side look like?

In-Band Attacks

- Premise: Actually, the CyberWarfare proponents don't talk about this one, either - ***why?***
- Reality:
  - Launching an attack ***via*** a network you are in the middle of ***destroying*** is not easy!
    - This is why most security management networks are two-tier!

In-Band Attacks *(cont)*

- If you can:
  - Remotely reconfigure routing on a 30-subnet, 4,000 node network ***without***
    - Getting disconnected
    - Accidentally partitioning a network so you can no longer get to it
    - Using a centralized network management station
    - Being detected

…then you may be “tall enough” to consider CyberWarfare as a career

(Or make millions by managing an ISP)

System Administration

- Premise: Actually, the CyberWarfare proponents don't talk about this one, *either* - ***why?***
  - Reality:
    - Fundamentally, the problem of ***taking over and destroying*** a network is a problem of approximately the same magnitude of ***managing*** that network
    - We've discovered that is a hard problem
    - Why are we so willing to ***assume*** that the CyberWarriors are going to be so ***gosh-darned*** skillful?

Traceability

- Premise: Actually, the CyberWarfare proponents don't talk about this one, *either* - ***why?***
- Reality:
  - For a military/political attack to be worth doing, it inherently must convey ***value*** to the ***attacker***
    - I.e.: A successful attack points towards a likely beneficiary
    - Finding out who shot an arrow is not hard!
  - This is fundamentally a very different dynamic than the non-ideological/apolitical hack attack

Philosophical Responses

- When I argue this some proponents of CyberWar respond:
  - *Everything* can be represented as information therefore warfare inherently has an information component
    - To which I respond, “Well, duh. That means Alexander the Great practiced CyberWar?”
  - *Eventually* everything will be computerized therefore all war will be computerized, too
    - To which I respond, “Infantry will still be carrying bayonets in 3000AD”

Conclusion

- Will there be CyberWar?
  - Sure, eventually (3000AD?)

  …but right now it's mostly a sales tool for security products companies and consultants
- In order for CyberWar to become real
  - We'll need computers to become a few orders of magnitude more ubiquitous
  - We'll need systems administration to become a few orders of magnitude better
    - It will have to be centralized, standardized, and ***insecure***