Quantum Computing: Security Implications

Robert M. Slade, MSc, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca,
rslade@gmail.com

http://en.wikipedia.org/wiki/Robert_Slade
http://www.victoria.tc.ca/techrev/rms.htm
http://twitter.com/rslade
http://fibrecookery.blogspot.com
https://is.gd/RotlWB

Quantum Computing: Security Implications

Rob Slade

p-1@shaw.ca
rslade@vcn.bc.ca
rslade@gmail.com

https://is.gd/RotlWB

http://twitter.com/rslade/

A little introduction ...

http://itsecurity.co.uk/2016/09/security-implications-quantum-computing/

http://itsecurity.co.uk/2016/09/cryptography-quantum-computing/

Do we understand quantum computing?

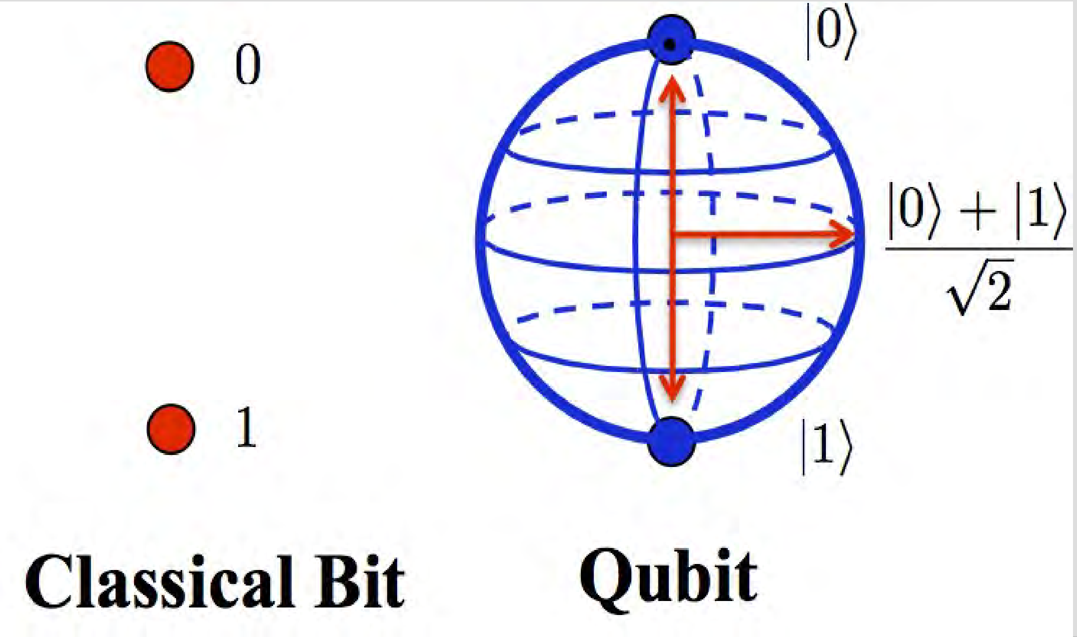
This isn't right.
It isn't even wrong.

- Wolfgang Pauli, on a paper submitted by a physicist colleague

Quantum introduction (very small)

Concepts

- Qubit
- Superposition



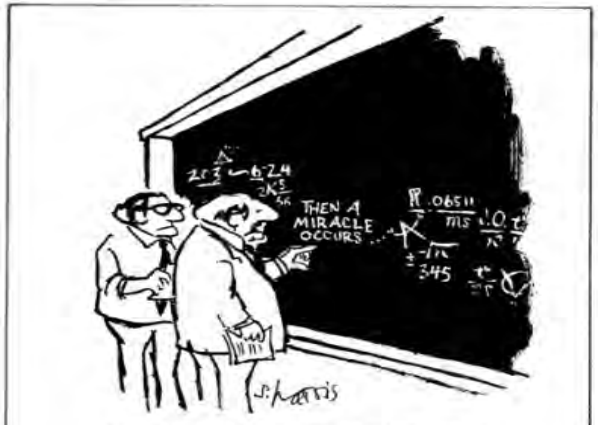
Quantum introduction (very small)

Concepts

- Entanglement
  - observer effect

Quantum introduction (very small)

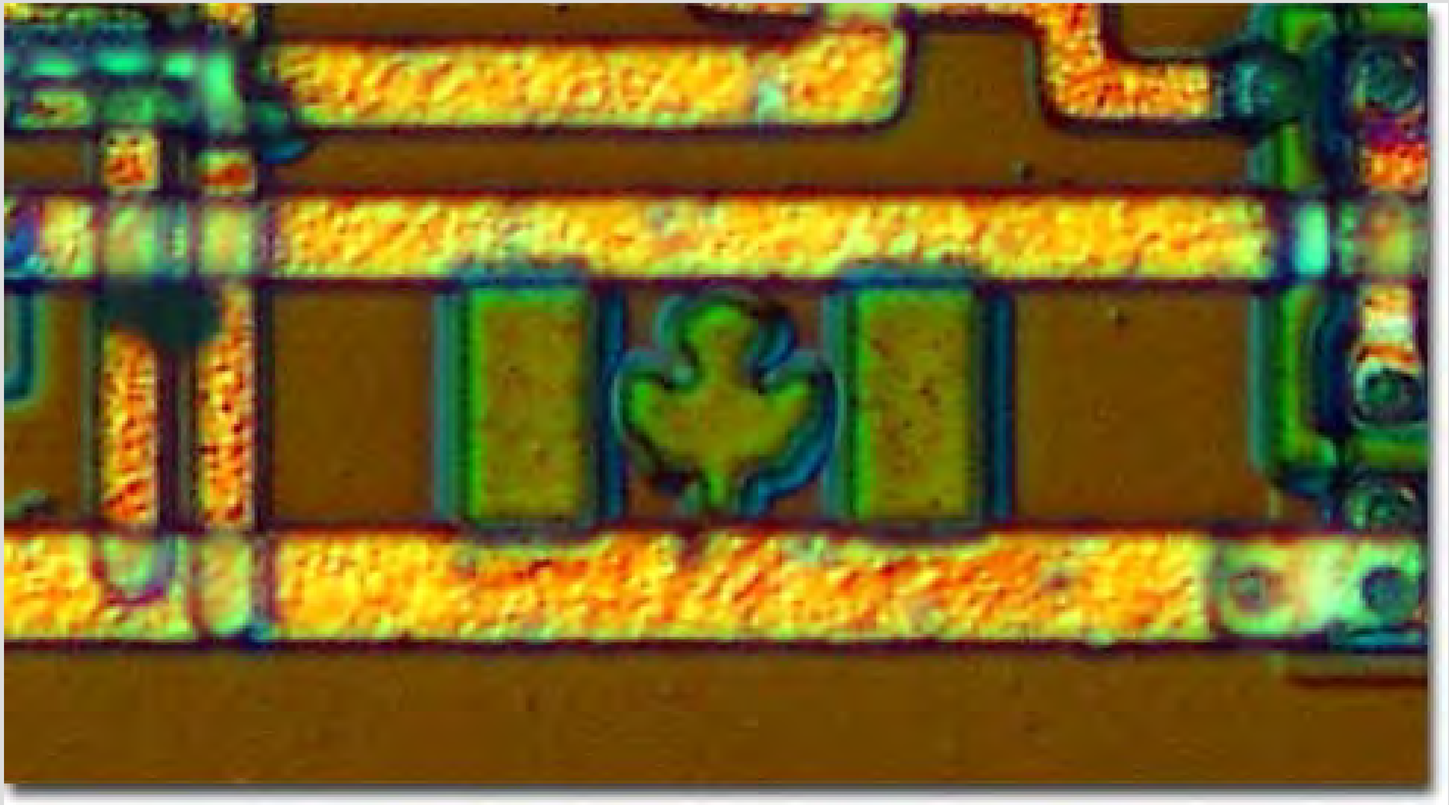
- “If someone says that he can think or talk about quantum physics without becoming dizzy, that shows only that he has not understood anything whatever about it.”
  - Niels Bohr



“I think you should be more explicit here in step two.”

Quantum Computing (1)

- Quantum computer
  - quantum tech, traditional operation
  - smaller, faster
    - quantum size range



Quantum Computing (1a)

- Turing
    - universal computer
    - irreversible computations
        - power

Quantum Computing (2)

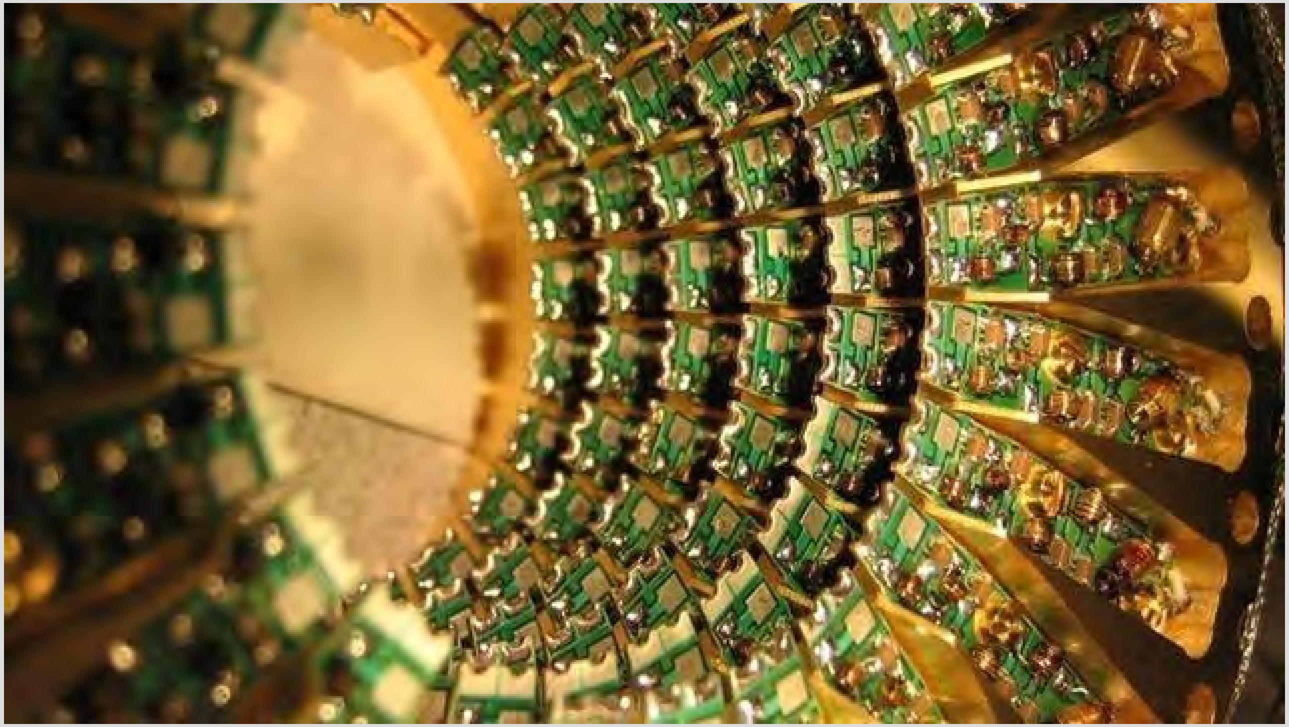
- Quantum cryptography (real)
  - photon polarization
    - angular polarization
    - detector angle
    - public exchange of angle but not value
  - photon entanglement
    - eavesdropping detection

(pause for demo) (no, we don't have time)

- Quantum decryption
  - hypothesized

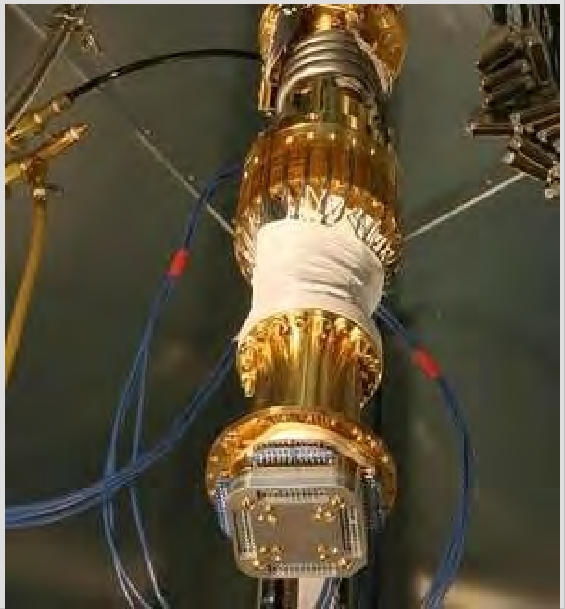
Quantum Computing (3)

- Quantum computing
  - computing device or processor
  - analogue computer
    - not digital?



Analogue Computers

- Spaghetti computing
  - parallel sorting
  - special purpose/application
- Slide rule
  - exact computation
    - imprecise reading
- Adiabatic quantum computer
  - least energy = best answer
    - least path, best comparison, simulation
  - D-Wave Orion, 1, 2
  - 3?

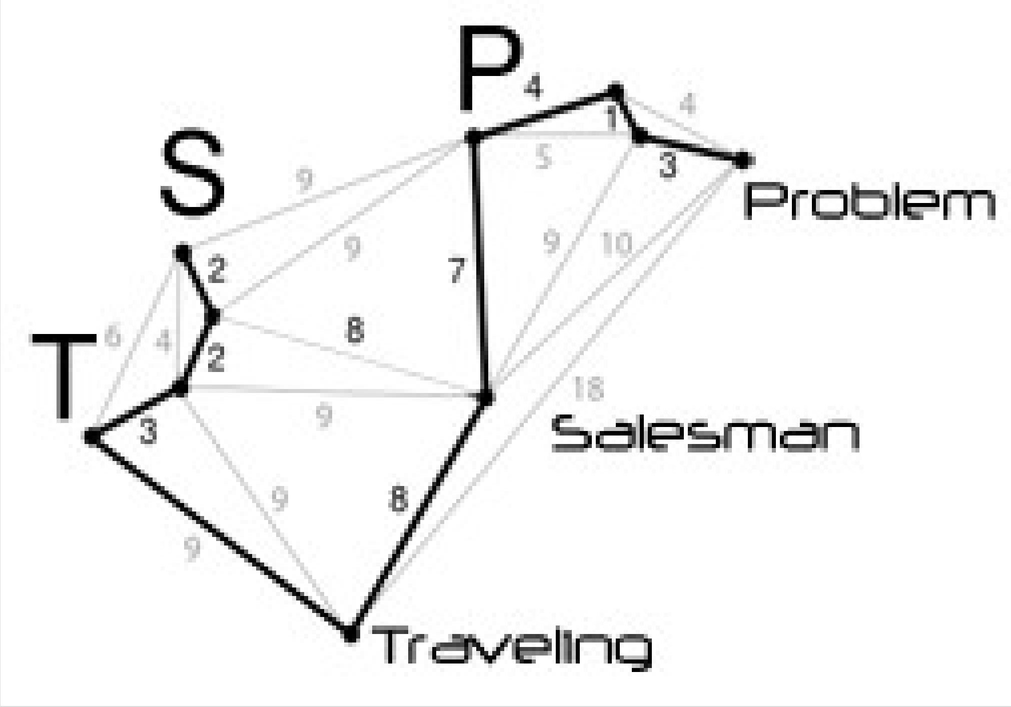


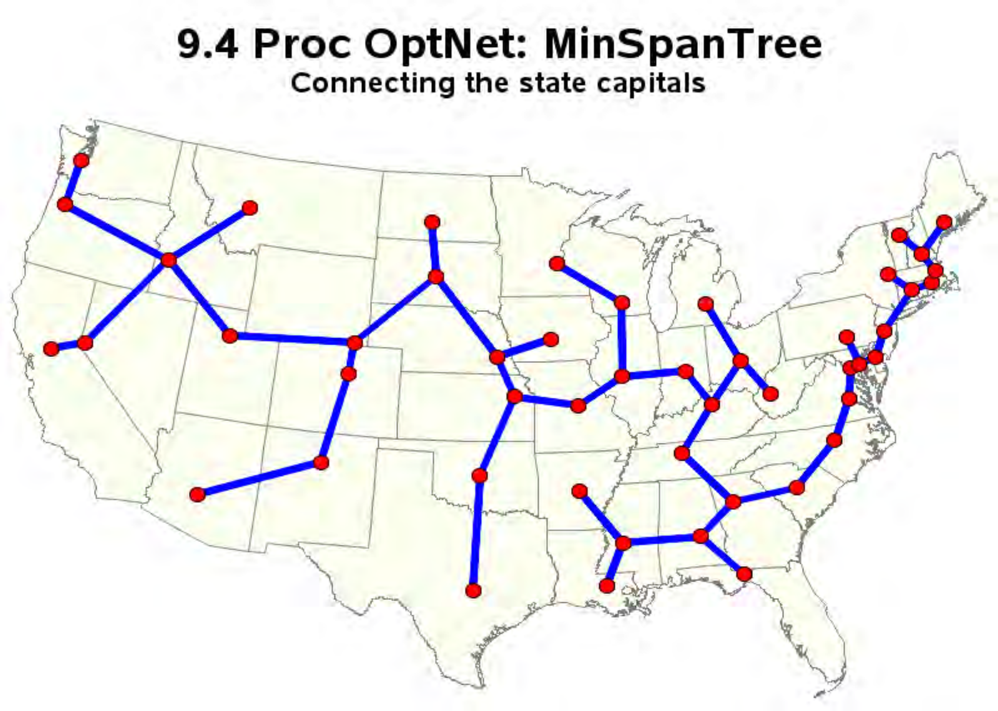
Applications and Implications

- by security domain (no, I'm not pushing (ISC)^2 jargon)
- general functions
  - least path
  - simulation
  - pattern matching

Applications and Implications

- least path
  - Traveling Salesman Problem
  - scheduling, efficiency studies, multiple requirements
  - NP-complete, non-convergent, Ising model

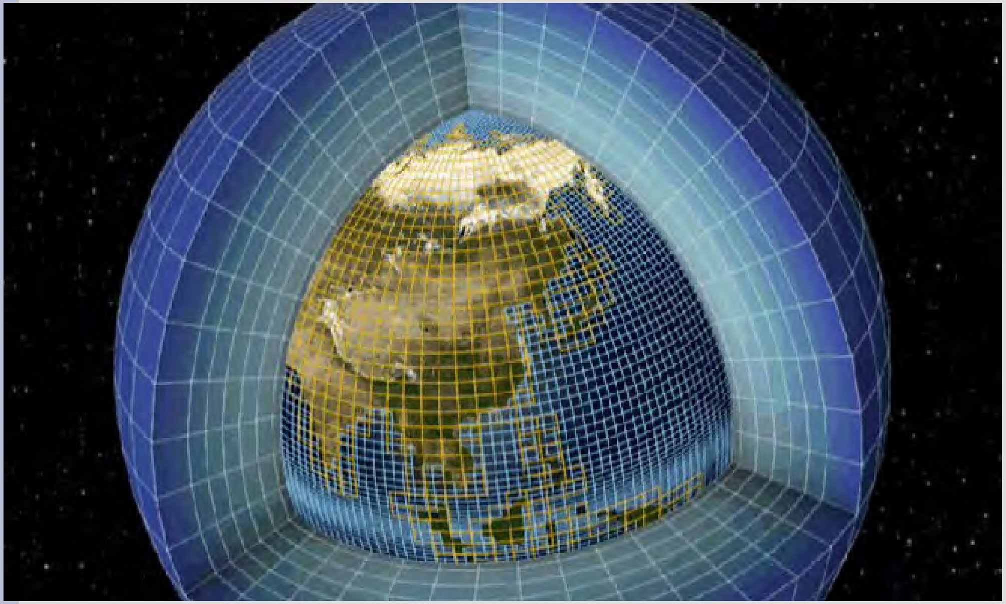


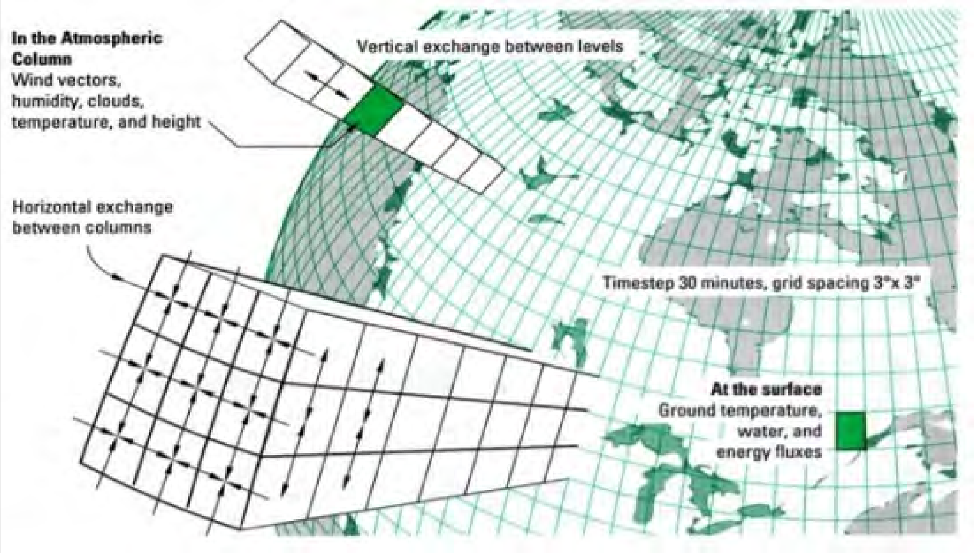


Applications and Implications

– simulation

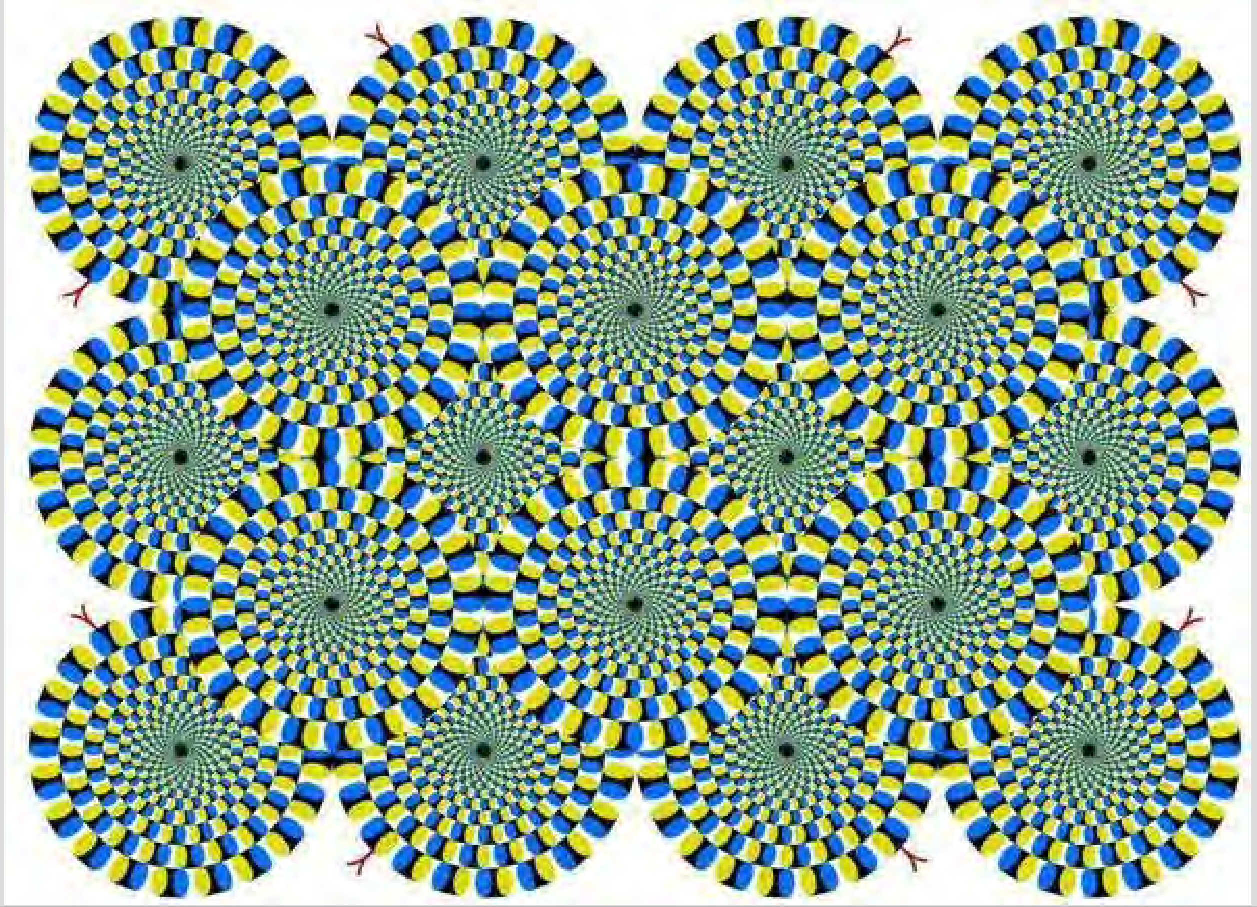
- climate models




In the Atmospheric Column
Wind vectors, humidity, clouds, temperature, and height
Vertical exchange between levels
Horizontal exchange between columns
Timestep 30 minutes, grid spacing 3°x 3°
At the surface
Ground temperature, water, and energy fluxes

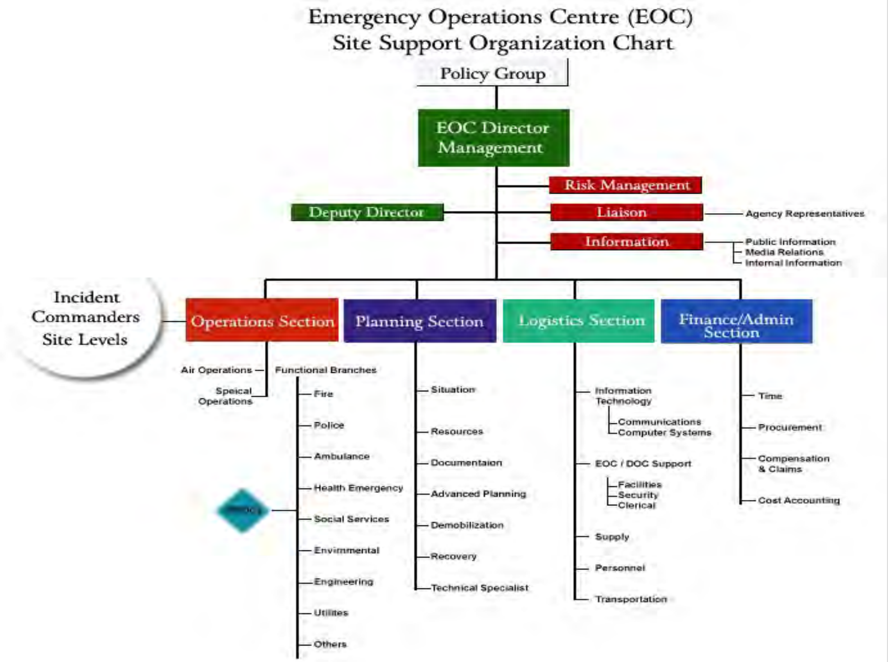
Applications and Implications

- pattern recognition
  - people are good, computers are bad
  - data reduction and representation



Security management

- risk management (shortest path)
  - what if - cost vs benefit



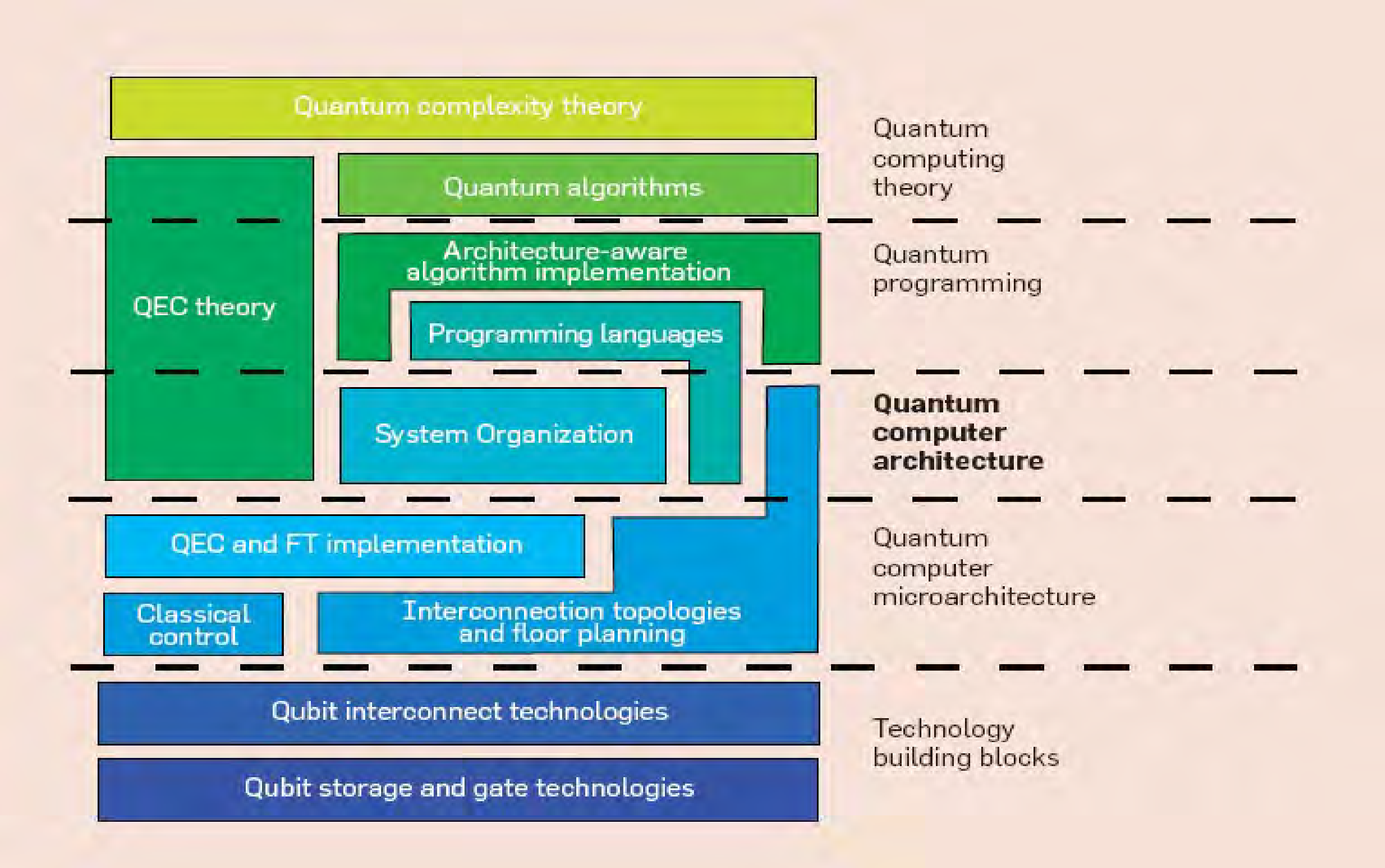
Security management

- information classification (pattern matching)
- risk assessment required
  - investing, or not, in quantum computing

F.U.D.
The Information Classification steering group has been disbanded.
Why?
No one had a high enough clearence to read the minutes.

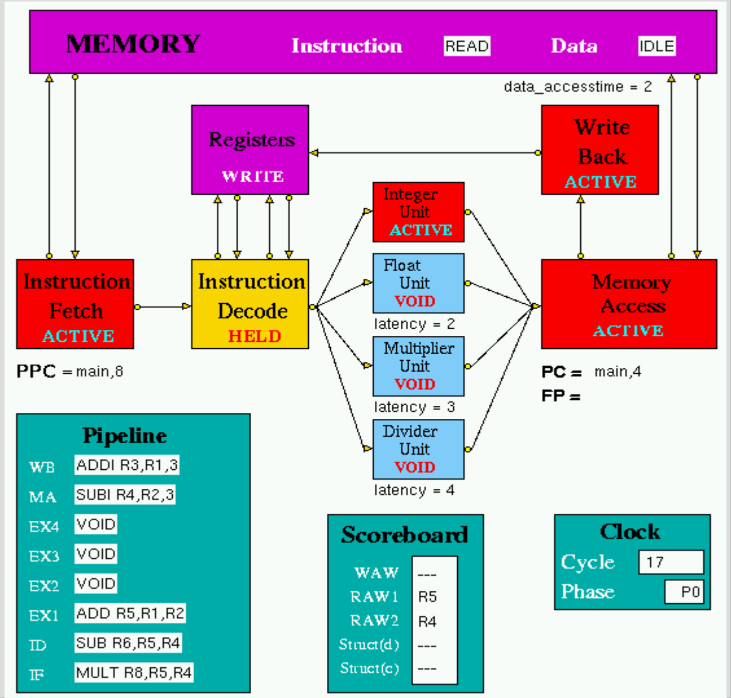
Security architecture

- new architectures, new vulnerabilities


Quantum complexity theory
Quantum algorithms
Quantum computing theory
QEC theory
Architecture-aware algorithm implementation
Programming languages
Quantum programming
System Organization
Quantum computer architecture
QEC and FT implementation
Classical control
Interconnection topologies and floor planning
Quantum computer microarchitecture
Qubit interconnect technologies
Qubit storage and gate technologies
Technology building blocks

Security architecture

- simulation of vulnerabilities and protections
- quantum devices and noise
  - D-Wave Orion voting, error checking
- quantum error correction (recent)
  - fault tolerant computing



Access control

- biometrics (pattern matching)

Access control

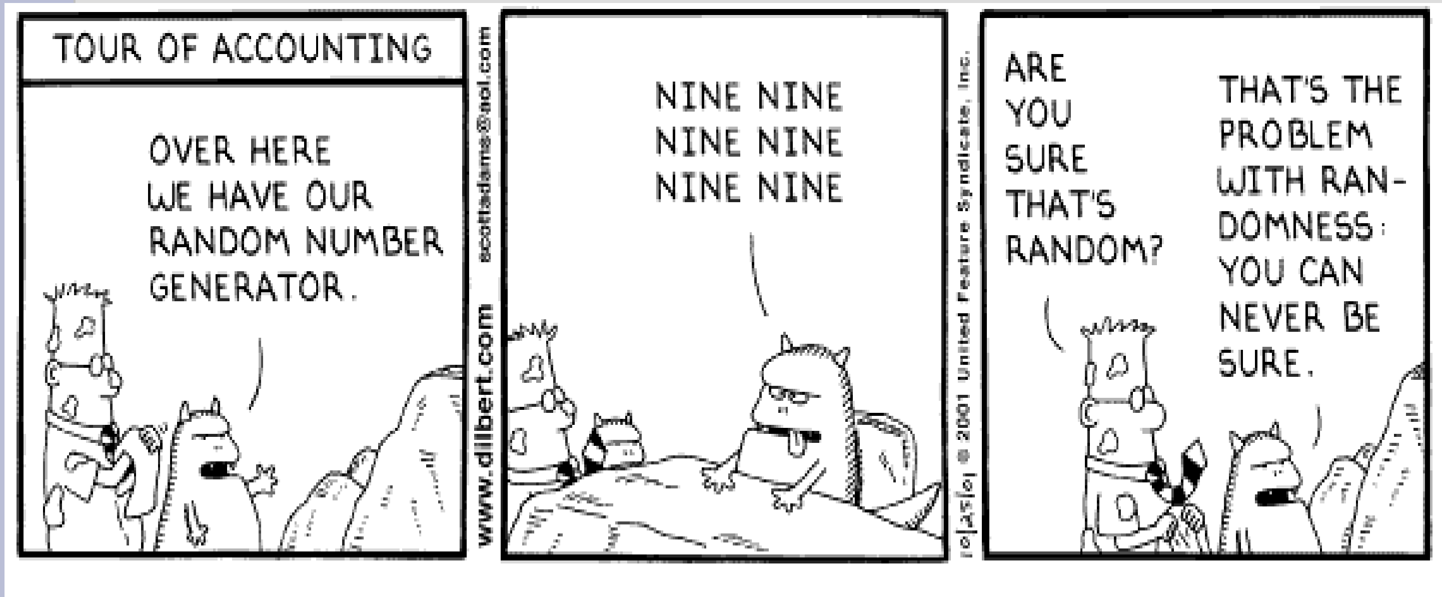
- information flow and covert channel analysis (least path/simulation)
- intrusion detection (pattern matching)

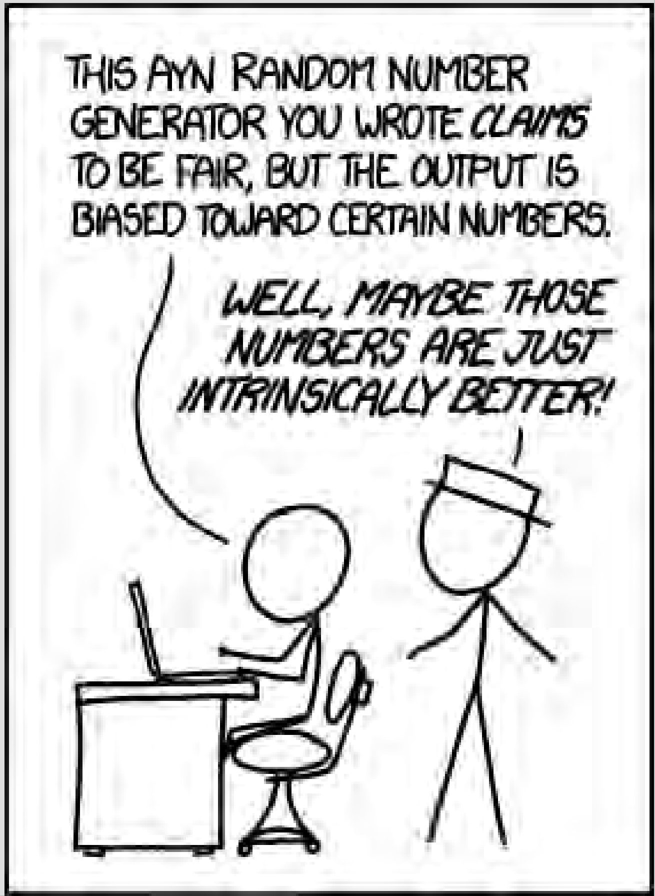
Cryptography

- quantum communications/encryption/key negotiation/eavesdropping detection
- parallel decryption
- new algorithms
  - tractable by neither classical nor quantum

Cryptography

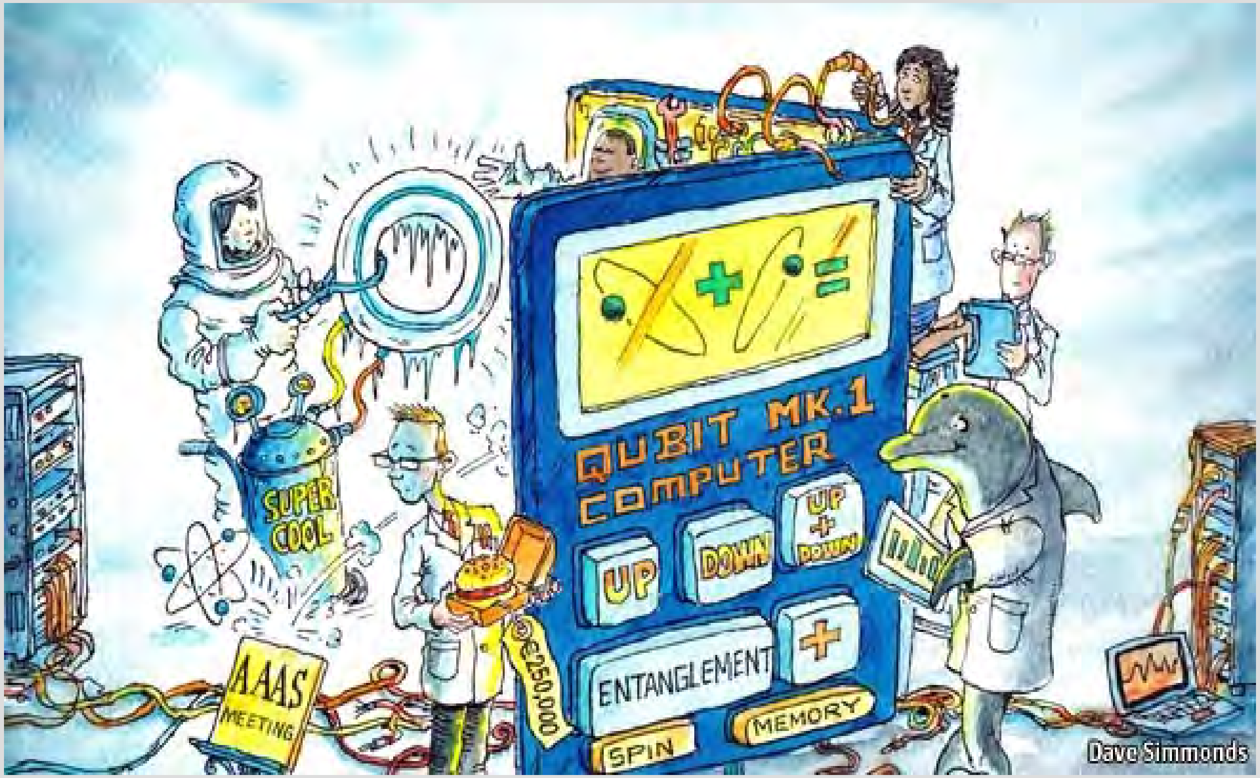
- quantum devices and generation of randomness
- analysis of implementation problems (simulation)


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
10/25/01 © 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.


THIS AYN RANDOM NUMBER GENERATOR YOU WROTE CLAIMS TO BE FAIR, BUT THE OUTPUT IS BIASED TOWARD CERTAIN NUMBERS.
WELL, MAYBE THOSE NUMBERS ARE JUST INTRINSICALLY BETTER!

Physical

- noise, RFI/EMI interference
- temperature
  - room temp 100x > interstellar space
  - interstellar space 1000x > Orion device



Physical

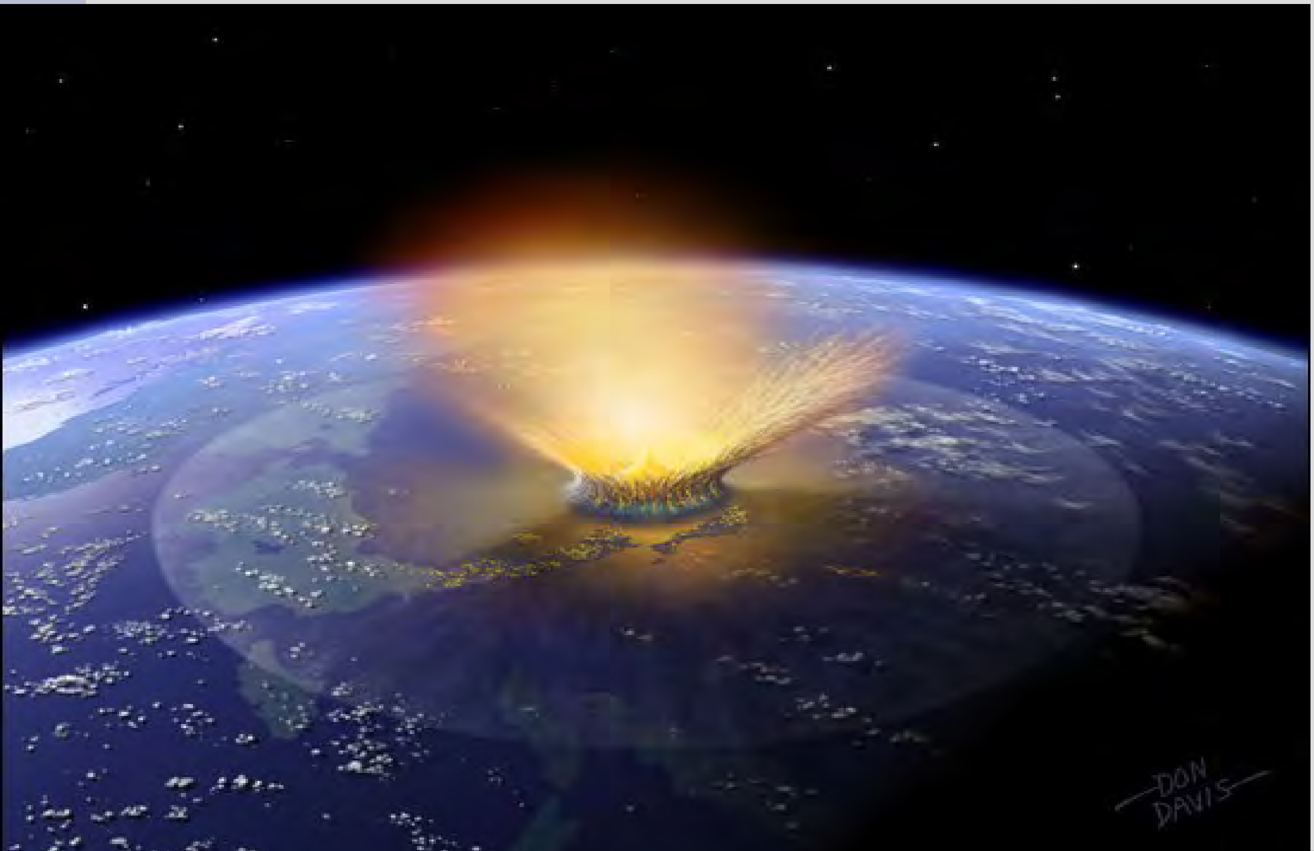
- special costs, protections for devices
- physical access control (biometrics)

BCP

- Business Impact Analysis (least path)
- testing of BC plans (simulation)

OK, THEN IT'S SETTLED, LOUIE. SINCE YOU'RE THE TALLEST, YOU JUST KEEP LOOKING UP, AND WHEN YOU SEE THE ASTEROID HEADING OUR WAY, YOU YELL, "DUCK!"
creators.com
© 2015 Leigh Rubin!
leigh@rubescartoons.com
6-17

The Cretaceous Disaster Preparedness Committee

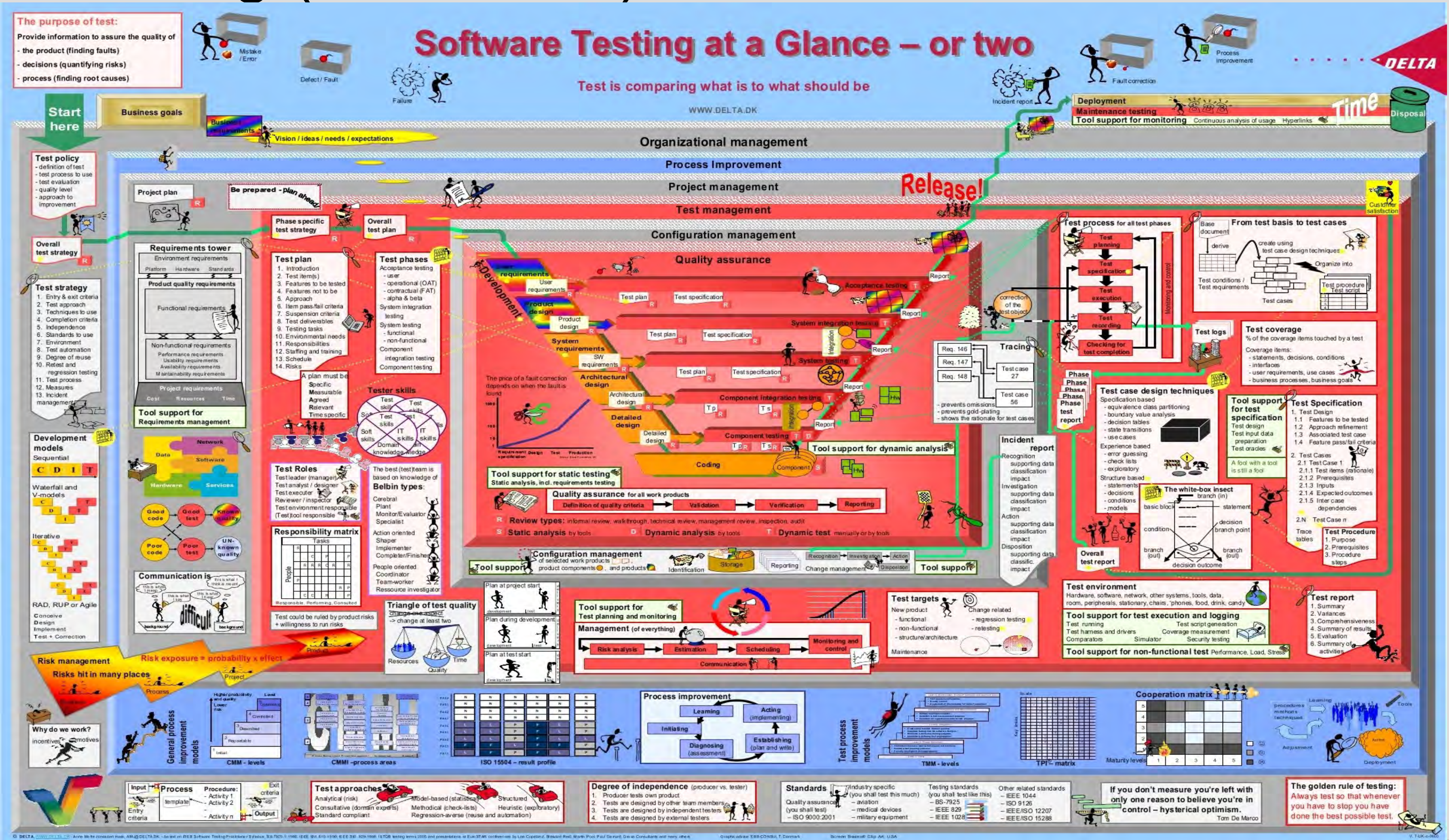


BCP

- disaster management
  - direction of resources to maximum effect
- continuity of operations for special devices
  - damage if power/cooling fails

Applications security

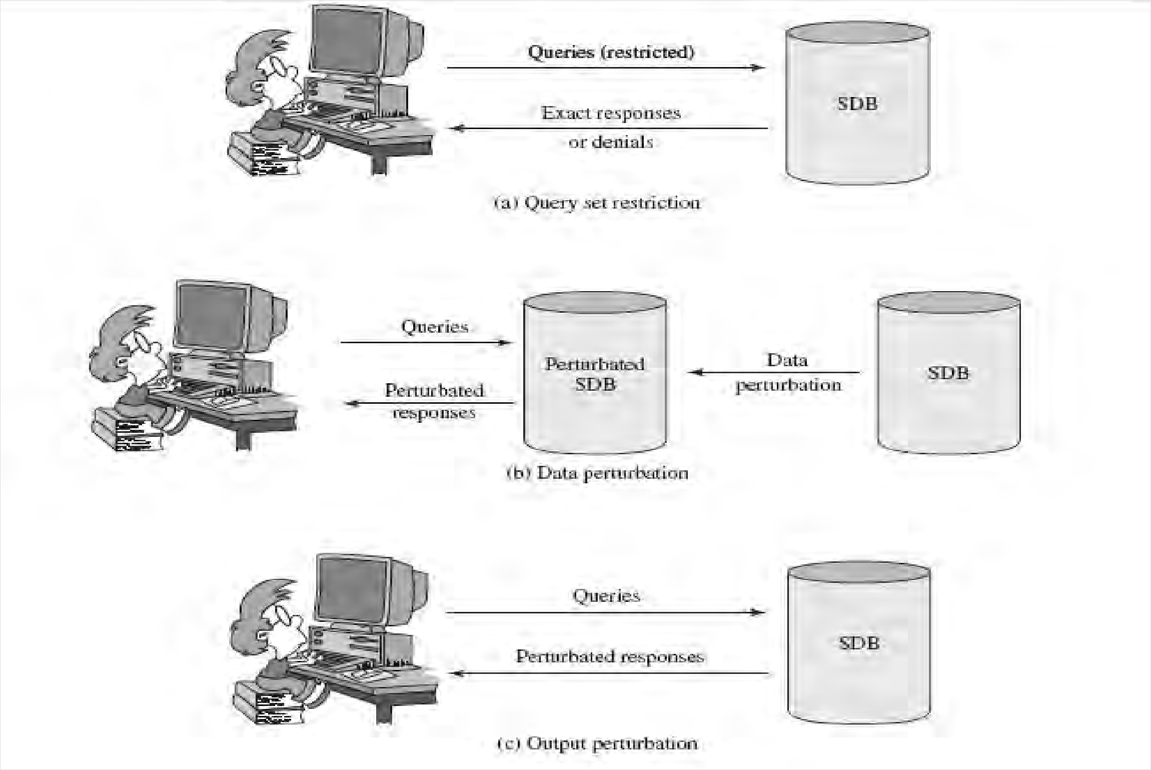
- testing (simulation)



The purpose of test:
Provide information to assure the quality of
- the product (finding faults)
- decisions (quantifying risks)
- process (finding root causes)
Software Testing at a Glance – or two
Test is comparing what is to what should be
WWW.DELTA.DK
DELTA
Mistake / Error
Defect / Fault
Failure
Incident report
Fault correction
Process improvement
Start here
Business goals
Vision / ideas / needs / expectations
Deployment
Maintenance testing
Tool support for monitoring
Time
Disposal
Organizational management
Process Improvement
Project management
Test management
Configuration management
Quality assurance
Release!
Test policy
Project plan
Be prepared - plan ahead!
Phase specific test strategy
Overall test plan
Overall test strategy
Requirements tower
Test strategy
Test plan
Test phases
Development
Acceptance testing
System integration testing
System testing
Component integration testing
Component testing
Coding
Tracing
Test process for all test phases
From test basis to test cases
Test coverage
Test logs
Test case design techniques
Tool support for test specification
Test Specification
Incident report
Tester skills
Test Roles
Belbin types
Responsibility matrix
Tool support for static testing
Tool support for dynamic analysis
Quality assurance for all work products
Review types
Static analysis
Dynamic analysis
Dynamic test
Development models
Communication is difficult
Triangle of test quality
Tool support for Test planning and monitoring
Management (of everything)
Risk analysis
Estimation
Scheduling
Monitoring and control
Communication
Test targets
Test environment
Tool support for test execution and logging
Tool support for non-functional test
Test report
Configuration management
Tool support
Overall test report
Risk management
Risks hit in many places
Risk exposure = probability x effect
Why do we work?
General process improvement models
CMM - levels
CMMI - process areas
ISO 15504 - result profile
Process improvement
Test process improvement models
TMM - levels
TPI - matrix
Cooperation matrix
Process
Test approaches
Degree of independence
Standards
If you don't measure you're left with only one reason to believe you're in control – hysterical optimism.
Tom De Marco
The golden rule of testing:
Always test so that whenever you have to stop you have done the best possible test.

Applications security

- database analysis (pattern matching)
  - cost (privacy) vs benefit (safety)
- database aggregation problem analysis (pattern matching and simulation)



(a) Query set restriction

(b) Data perturbation

(c) Output perturbation

Applications security

- learning (pattern matching)
  - neural net augmented
  - check against neural net superstitious learning

> When we write programs that learn, it turns out that we do and they don't.
>
> - Alan J. Perlis

Applications security

- check against expected
  - impossible to compute by classical methods

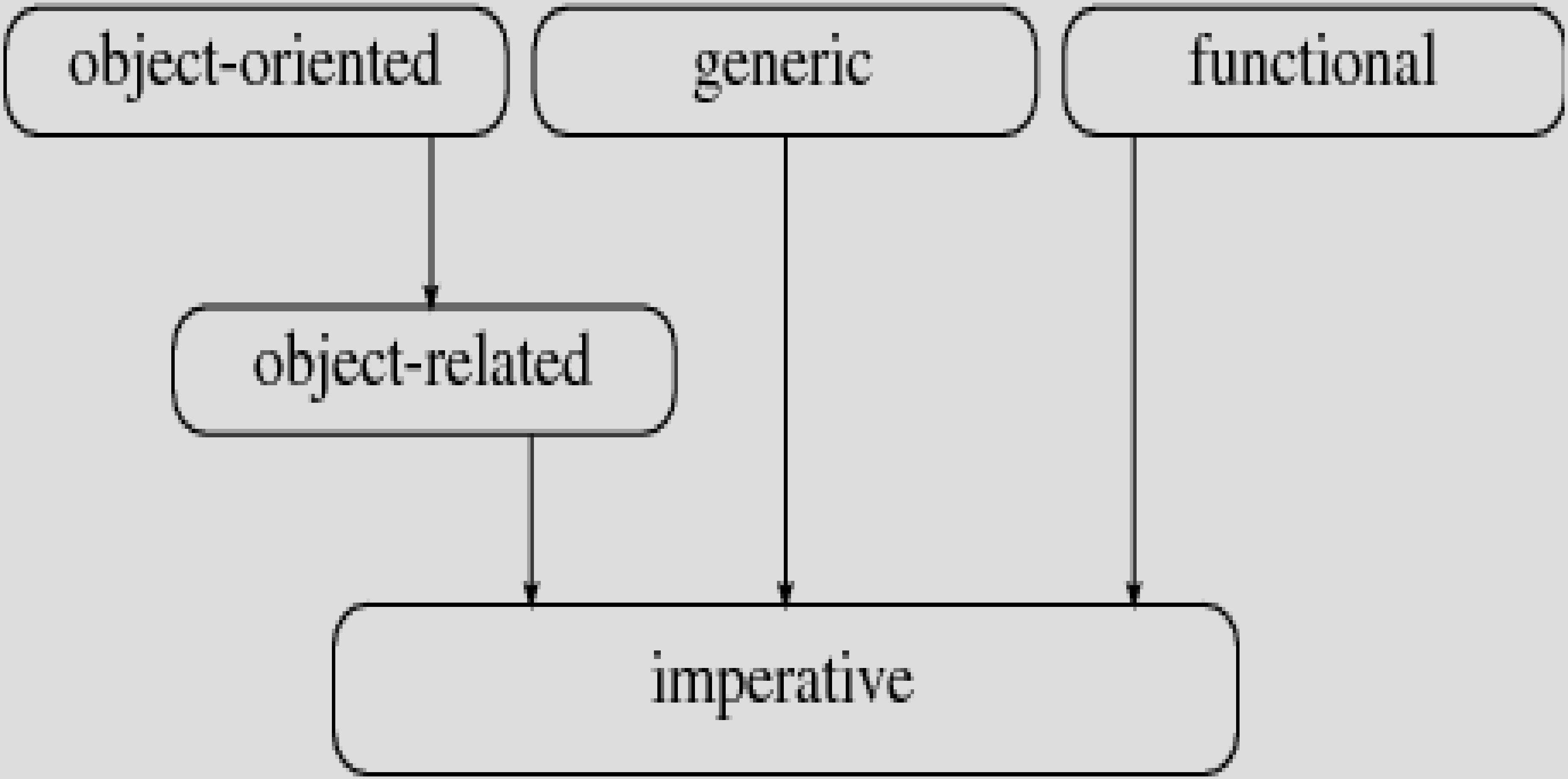
Applications security

- malware/botnet detection, (pattern matching)
  - operation/control/ownership

IT CAN'T HURT TO OPEN ONE LITTLE ATTACHMENT, CAN IT ?...
PANDORA'S INBOX
©2009 COVERLY 3-25
DIST. BY CREATORS SPEEDBUMP.COM

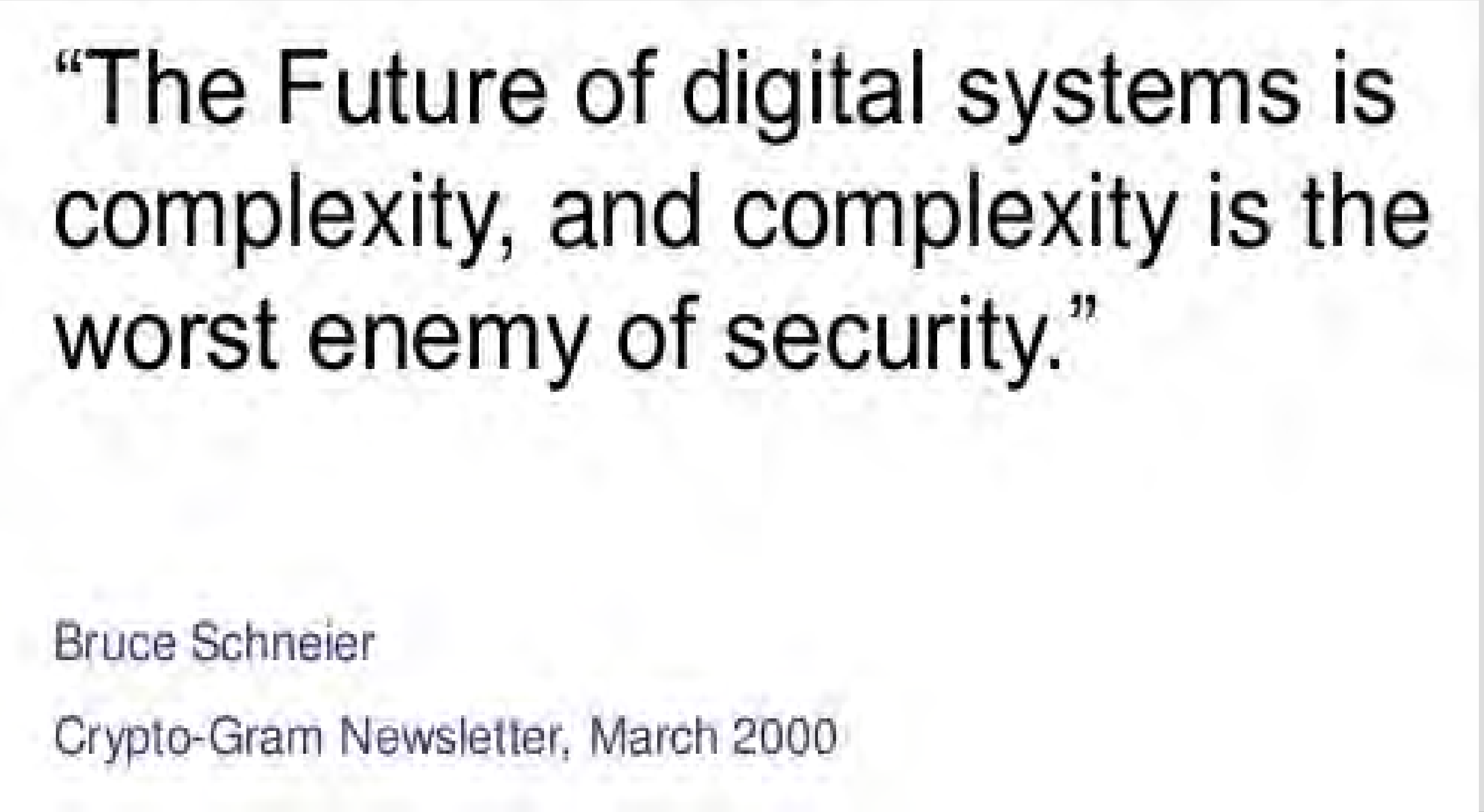
Applications security

- completely new paradigms in programming



Operations security

- combinations of classical and quantum devices and operations
  - complexity, troubleshooting



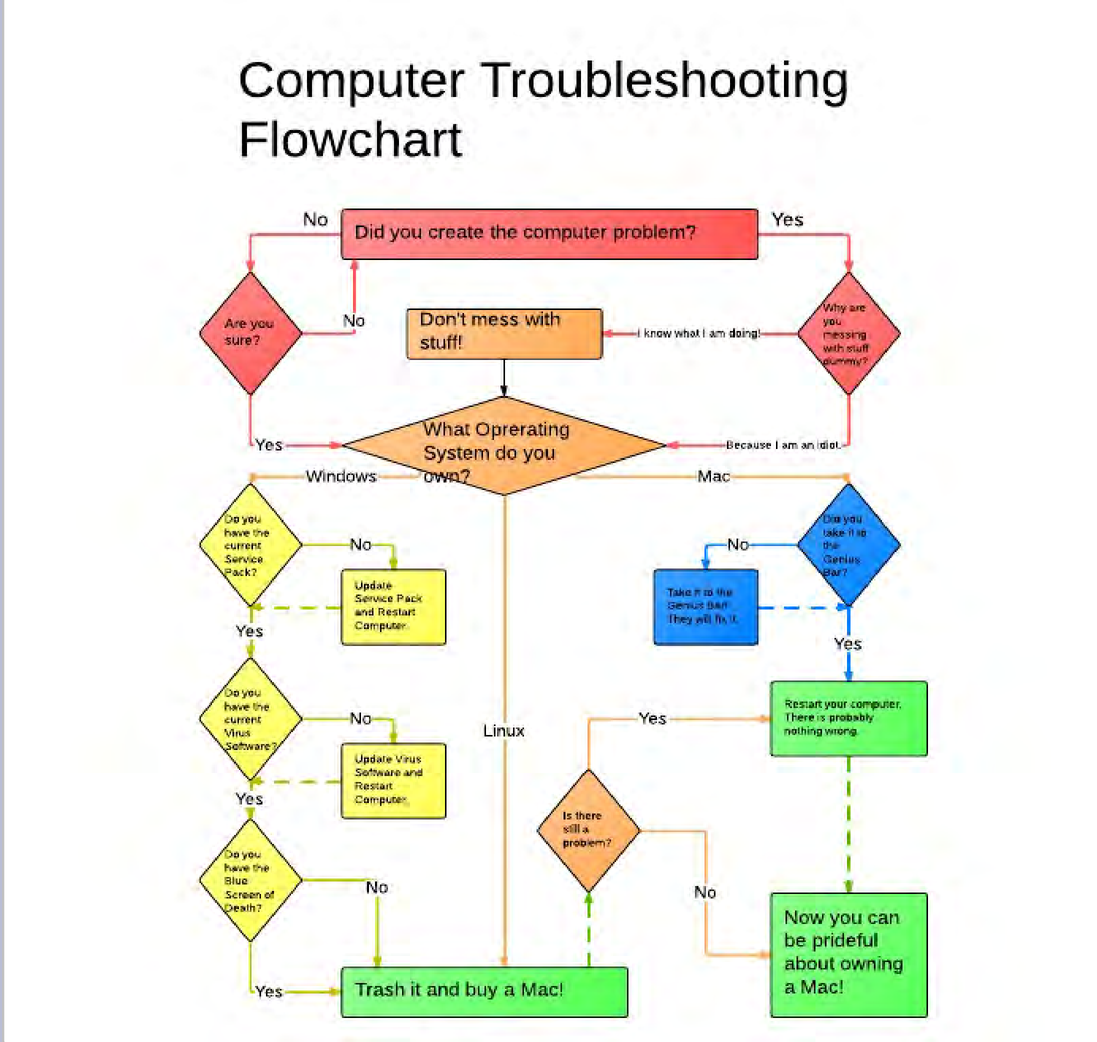
"The Future of digital systems is complexity, and complexity is the worst enemy of security."

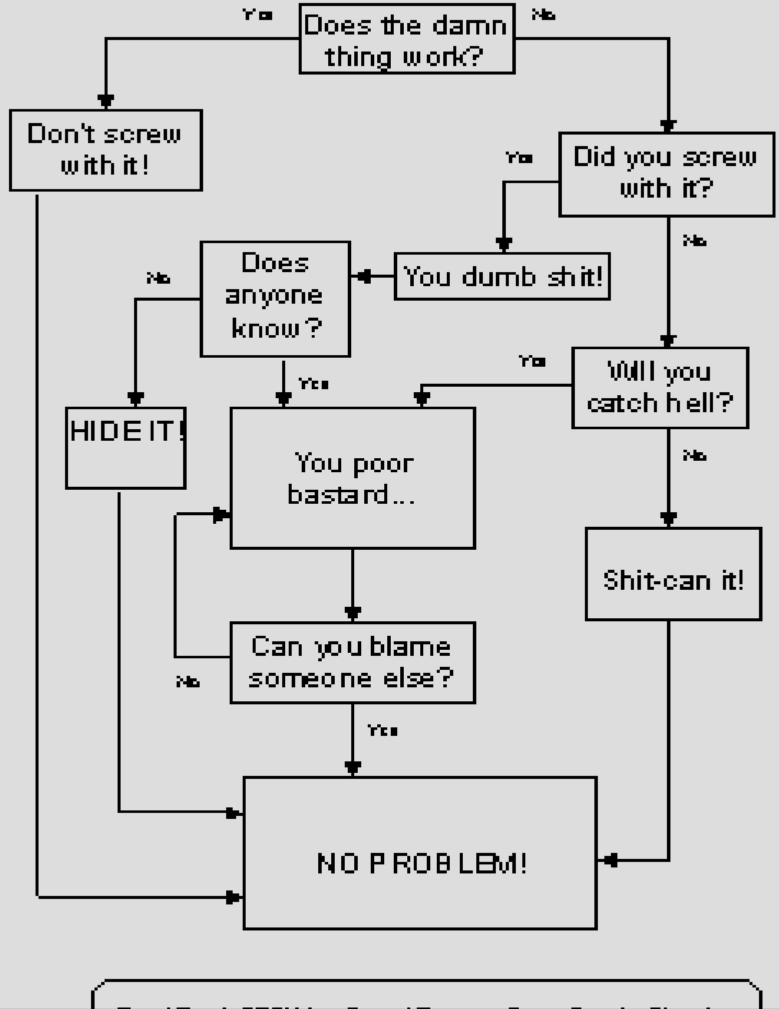
Bruce Schneier

Crypto-Gram Newsletter, March 2000

Operations security

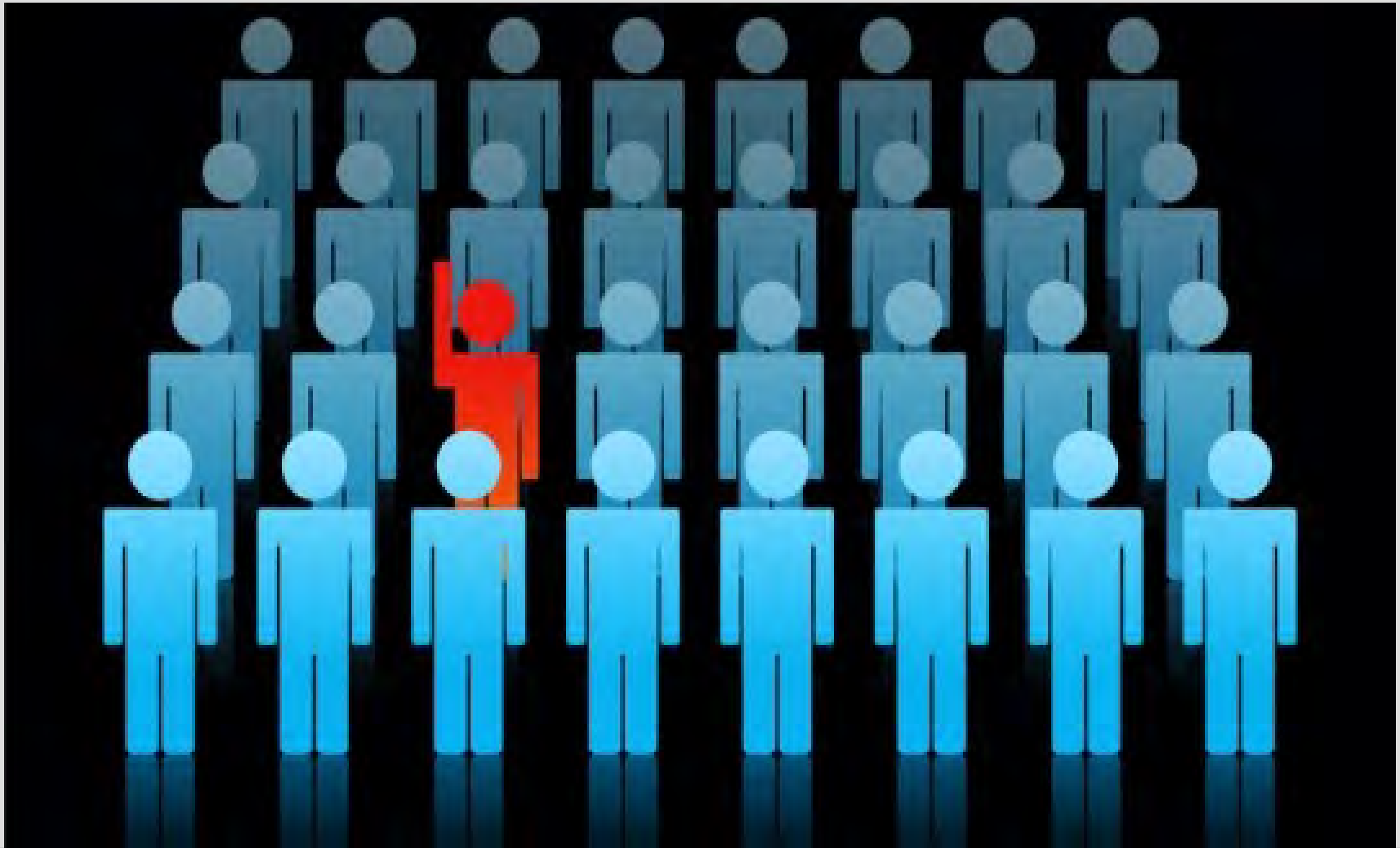
- troubleshooting (simulation)


Computer Troubleshooting Flowchart
Did you create the computer problem?
No
Yes
Are you sure?
No
Yes
Don't mess with stuff!
Why are you messing with stuff dummy?
I know what I am doing!
Because I am an idiot.
What Oprerating System do you own?
Windows
Mac
Linux
Do you have the current Service Pack?
No
Update Service Pack and Restart Computer
Yes
Do you have the current Virus Software?
No
Update Virus Software and Restart Computer
Yes
Do you have the Blue Screen of Death?
No
Yes
Trash it and buy a Mac!
Do you take it to the Genius Bar?
No
Take it to the Genius Bar! They will fix it.
Yes
Restart your computer. There is probably nothing wrong.
Is there still a problem?
Yes
No
Now you can be prideful about owning a Mac!



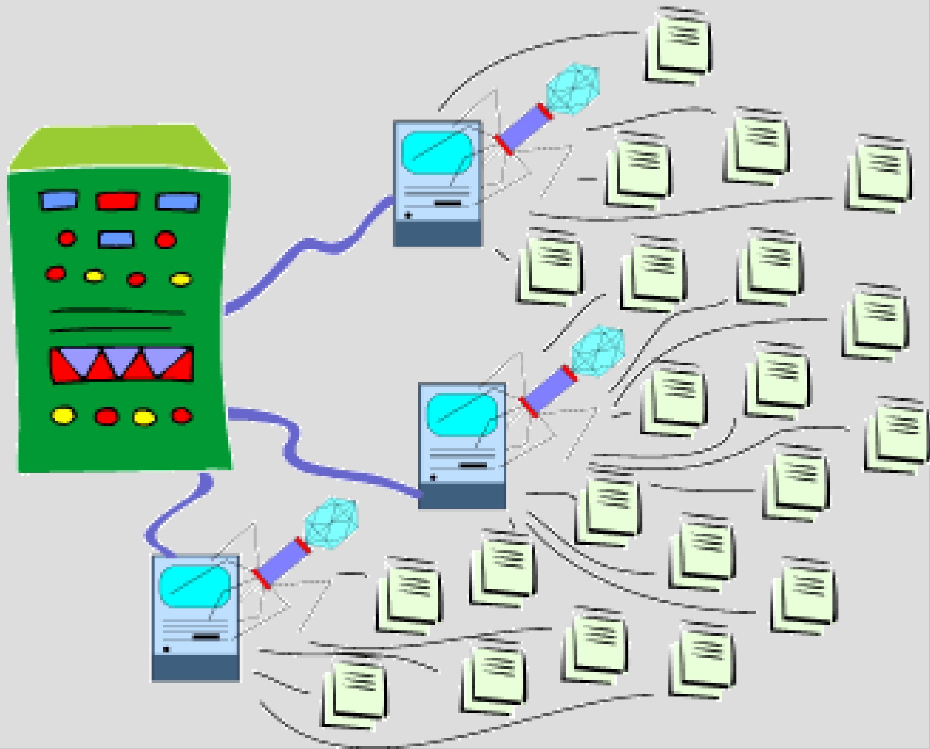
Operations security

- insider attack detection (pattern matching)



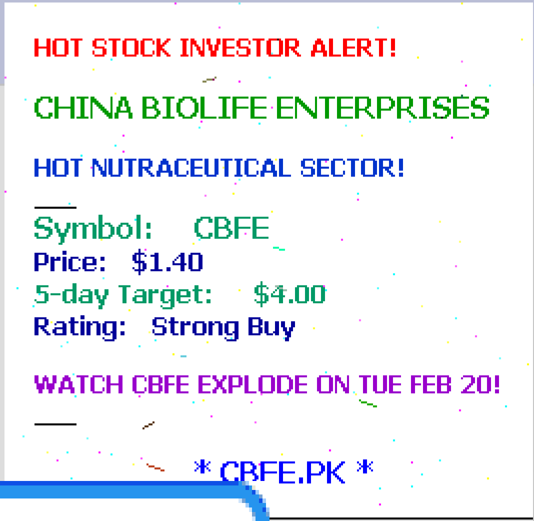
Telecommunications and networking

- Intrusion Detection Systems
- Botnet detection and assessment
  - Command & Control
  - ownership
  - “fast flux”
- Network attack analysis



Telecommunications and networking

- Spam
  - limitations even in Bayesian analysis



HOT STOCK INVESTOR ALERT!

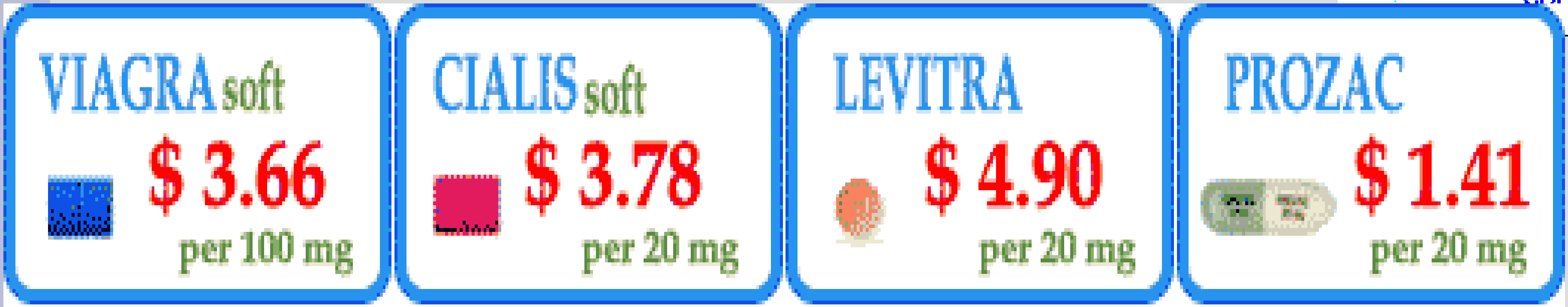
CHINA BIOLIFE ENTERPRISES

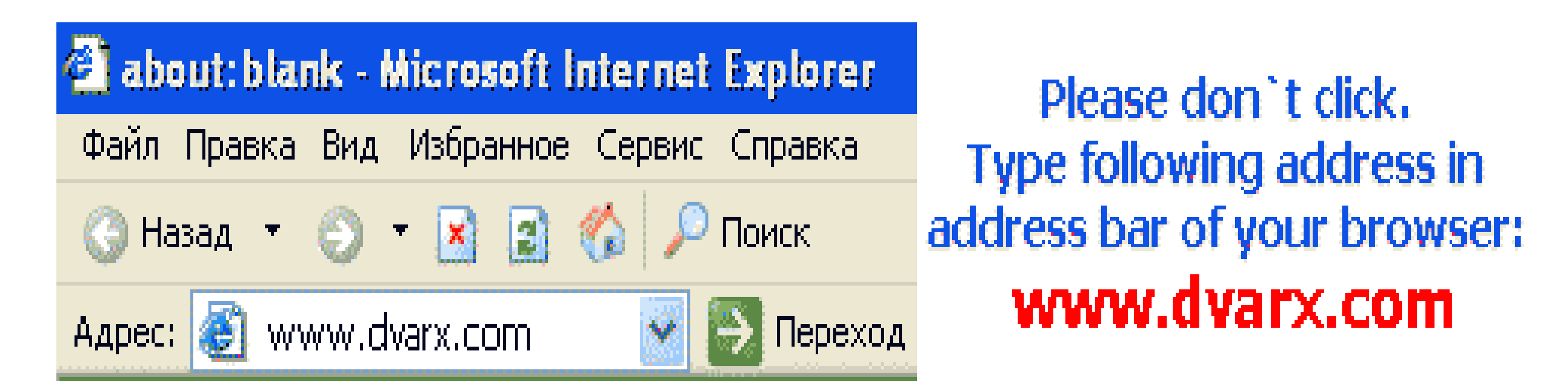
HOT NUTRACEUTICAL SECTOR!

Symbol: CBFE
Price: $1.40
5-day Target: $4.00
Rating: Strong Buy

WATCH CBFE EXPLODE ON TUE FEB 20!

* CBFE.PK *




about:blank - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад
Поиск
Адрес:
Переход

Адрес: www.dvarx.com

Please don`t click.
Type following address in address bar of your browser:
www.dvarx.com

Telecommunications and networking

- quantum encryption requires special channels
- quantum devices likely to be remote access

Telecommunications and networking

- More than one bit per photon
    - One test sent enough data for small graphic
        - (128 bits?)
- “continuously variable”
    - “analogue photon”?

Telecommunications and networking

- Quantum networks
  - https://scitechdaily.com/researchers-establish-the-first-entanglement-based-quantum-network/
  - What application?
- “Quantum LAN” may be engineering solution to problem of mesh connections necessary for massive numbers of qubits
  - “distributed quantum computer”?

Law and investigation

- new forensic analysis tools (pattern matching/simulation)
- presentation/acceptance in court problematic

Quantum Computing:
Security Implications

Robert M. Slade, MSc, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca,
rslade@computercrime.org

http://en.wikipedia.org/wiki/Robert_Slade
http://www.victoria.tc.ca/techrev/rms.htm
http://twitter.com/rslade
http://blogs.securiteam.com/index.php/archives/author/p1/
https://is.gd/RotlWB

Quantum Computing: Security Implications

Rob Slade

p-1@shaw.ca
rslade@vcn.bc.ca
rslade@gmail.com

https://is.gd/RotlWB

http://twitter.com/rslade/