

Big Data and Cyber Security

2016-03-16

MBIT - Monterey

Dr. Fred Cohen

This talk is about how big data is interacting with cyber security and what it is creating.


From the destruction of certain aspects of privacy to the ability to rapidly track and defeat malicious critical infrastructure attacks, the shame and promise of big data are coming to cyber security, whether we like it or not.

This introduction to and discussion of modern technologies, their limits, and their promise will engage you with spirited ideas, the realities of today, the limitations of the foreseeable future, and the implications to individuals and societies.

Don't miss this unique opportunity to see into and potentially impact the future.

Your speaker

- Past (partial list... details see all.net)
 - 1970s: Security HW&protocols
 - 1983: Computer virus defenses
 - ~90% of computers today
 - 1992: Information assurance in critical infrastructure protection
 - PCCIP → Sandia Natl. Labs
 - 1996: Deception for defense
 - → Deception Toolkit, Dazzler (DoD) Responder, patents
 - '90s: Digital forensics & ForensiX
 - 1998: Security simulation
 - 2000's: Burton Group
 - Sec & Risk Mgmt Strategies
 - Universities (1985-present)
- Present
 - CEO: Management Analytics
 - Partner: Fearless Security
 - Partner: Fearless Ridge
 - Lab director & Associate institute director: Webster University
 - President: Keiretsu forum - PB
 - Angel investor

<p>CyberSpace <u>Research and Development</u> <u>Information Protection</u> <u>Business spinoffs</u> <u>Litigation Support</u></p>	<p>Dr. Fred Cohen Trusted Adviser Since 1977 <u>Risk Management</u> <u>CyberSecurity</u> <u>Angel Investment</u></p>	<p>Angel Investment <u>Keiretsu Forum Chapter President</u> <u>Oasis Clean-tech Fund Advisory Board</u> <u>More than 30 Angel Investments</u></p>
<p>Current Companies <u>Management Analytics</u> <u>Fearless Security(with Chris Blask)</u> <u>Fearless Ridge (with Tom Ridge)</u> <u>TechVision Research (With Gary Rowe)</u></p>		<p>Investment Education <u>Innovation and Entrepreneurship</u> <u>Angel to Exit</u> <u>Keiretsu Forum Academy</u></p>
<p>Litigation Support <u>Expert Witness</u> <u>Digital Forensics</u> <u>Digital Diplomatics</u></p>	<p>CyberSpace Research Institute <u>Cyber Laboratories Director</u> <u>InterPares Trust Researcher</u> <u>Associate Institute Director</u></p>	<p>University <u>Webster Global Entrepreneurship</u> <u>Walker School of Business</u> <u>Angel Internship Program</u></p>

Outline

- What is “big data”?
 - How big is big?
 - Is “data” really just “data”?
- What is “cyber security”?
 - What is “cyber” about it?
 - What is “security”?
- How do they interact?
 - The who, what, where, why, when, and how of it
 - What does that mean to society?
- The past, present, and future
 - It's all about scale and business
 - Where do you want to go?

BIG

Big Data

- How big is big?
 - The “biggest” data I dealt with was in a legal matter as an expert witness:
 - ~15 trillion semi-structured records
 - ~10K average record size
 - Not organized in a database
 - Data fidelity questionable – often worse
 - No efficient way to copy, input, output, search, etc.
 - I regularly deal with evidence in legal matters involving ~1M relevant records
 - How big is your biggest big?
- Is “data” really just “data”?
 - We talk as if we didn't know that bit sequences have associated semantics
 - The semantics are the hard / really big part
 - Computational complexity is no longer theory as scale
 - Controlling how you do it is the real key to what it is you do

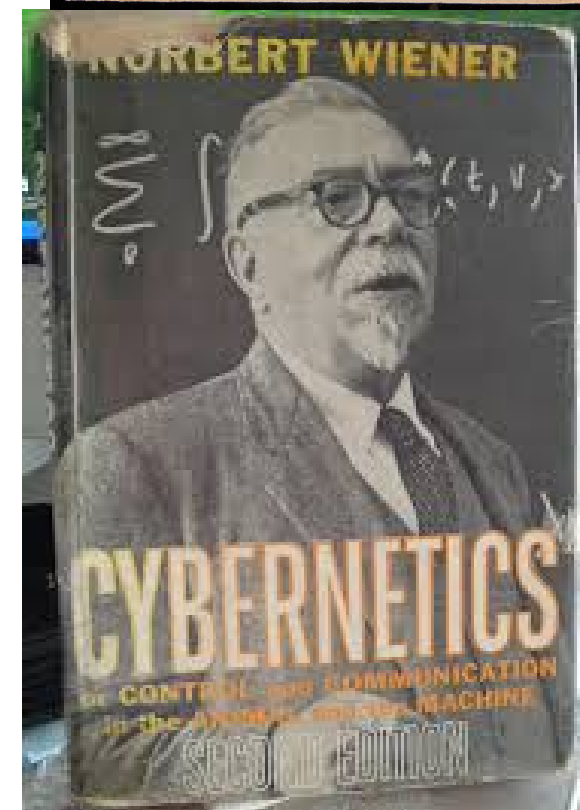
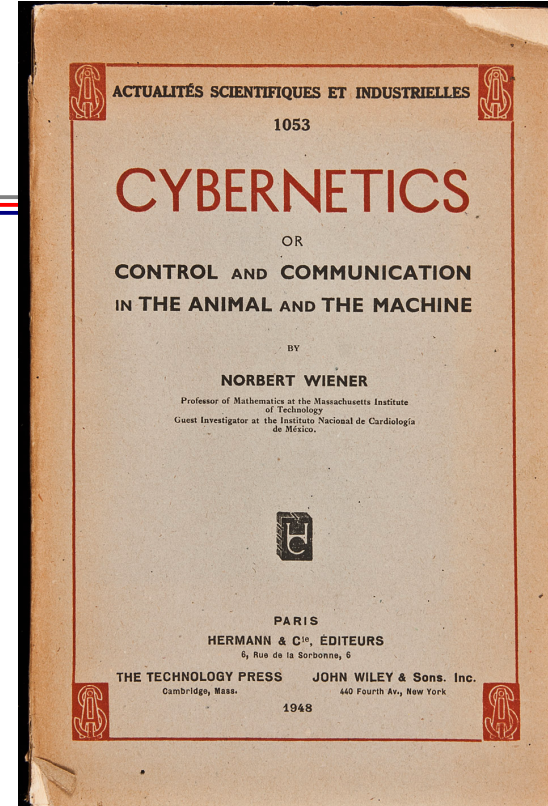
Outline

- What is “big data”?
 - How big is big?
 - Is “data” really just “data”?
- What is “cyber security”?
 - What is “cyber” about it?
 - What is “security”?
- How do they interact?
 - The who, what, where, why, when, and how of it
 - What does that mean to society?
- The past, present, and future
 - It's all about scale and business
 - Where do you want to go?



Cyber (space)

- “Cybernetics” (not dienetics!)
 - A book by Norbert Wiener circa 1948
 - “ the science of communication and control theory that is concerned especially with the comparative study of automatic control systems (as the nervous system and brain and mechanical-electrical communication systems)”
 - Greek kybernētēs pilot, governor (from kybernan to steer, govern) + English -ics [<http://www.merriam-webster.com/dictionary/cybernetics>]
- I used to pan it as an information technology term, but
 - Sensors now widely sense the physical world
 - Actuators commonly cause real-world effects
 - The operational technology (OT) is the control system
- → We live in a cybernetic (OT) world:
 - Cyberspace: The current frontier (hence the CRI)



Security

- Security used to be “the feeling of safety” (circa 1980s dictionary)
- Protection: “keep from harm”
- Now relatively meaningless as a term of art
- Covers a wide range of protective aspects

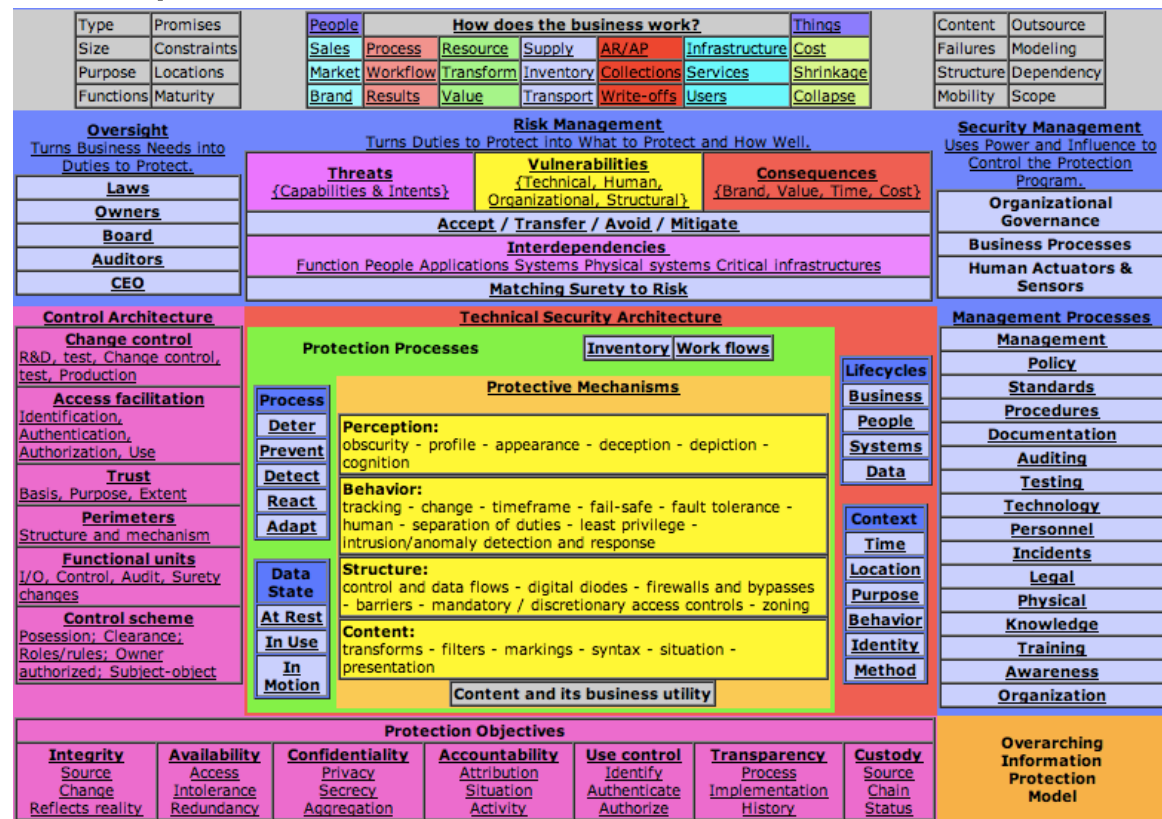


Fearless Security
Fearless Ridge All.Net

- Integrity
- Availability
- Confidentiality
- Accountability
- Use control
- Transparency
- Custody

- Operational risk management?

- No real definition → nebulous FUD



Outline

- What is “big data”?
 - How big is big?
 - Is “data” really just “data”?
- What is “cyber security”?
 - What is “cyber” about it? Let's use deep (cold) seawater
 - What is “security”? - to cool the computers
 - used to analyze global warming
- How do they interact?
 - The who, what, where, why, when, and how of it
 - What does that mean to society?
- The past, present, and future
 - It's all about scale and business
 - Where do you want to go?

The who, what, where, why, when, and how of it

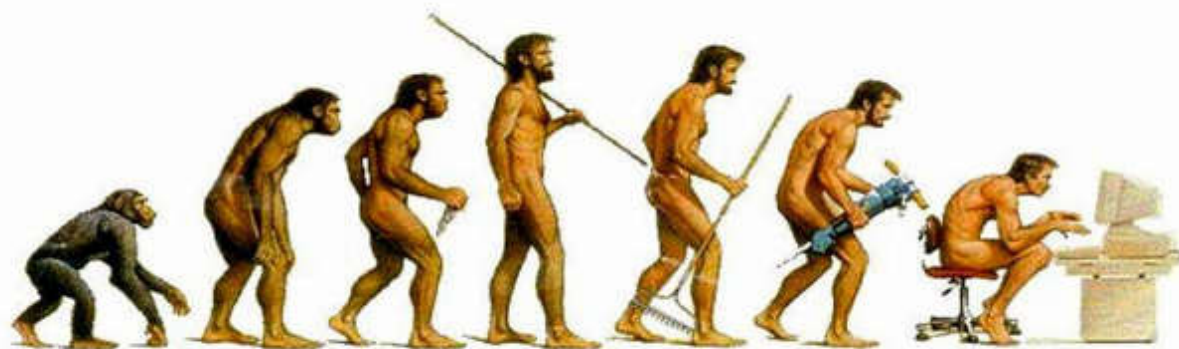
- Who:
 - Identity management and multi-point identification
- What:
 - Finer and finer grained activity control and tracing
- Where:
 - Location-based everything is getting easier and more precise
- When:
 - Time precision and accuracy is already excellent in many cases
- How:
 - Event sequence tracking and recording is now increasingly feasible
- Why?
 - Computers don't do “why”!

Now that we have all that, what do we do with it?

- Enormous potential for abuse
 - Unlimited surveillance
 - Large-scale cryptosystem defeat
 - Increasing the equities imbalance
 - Psychological & sociological abuse
 - Cyber warfare arms races
 - If WWII Germany had it ...
- Methodologies and limitations
 - Correlation is not causality
 - Guilt by association
 - Lack of provenance & traceability
 - Ignoring base rates
 - Visualization limitations
 - Confirmation not refutation
- Analytical promise and benefits
 - Detecting and stopping epidemics
 - Proof of software properties
 - Inconsistency/subversion detection
 - Situation anticipation & constraint
 - Process of elimination (traceback)
 - Automated detection and reaction
- Social implications
 - We are all always watched
 - There are no secrets from some
 - Unlimited use of human potential
 - Unlimited abuse if used badly
 - Ever-escalating cyberwarfare
 - Fear, Uncertainty, and Doubt

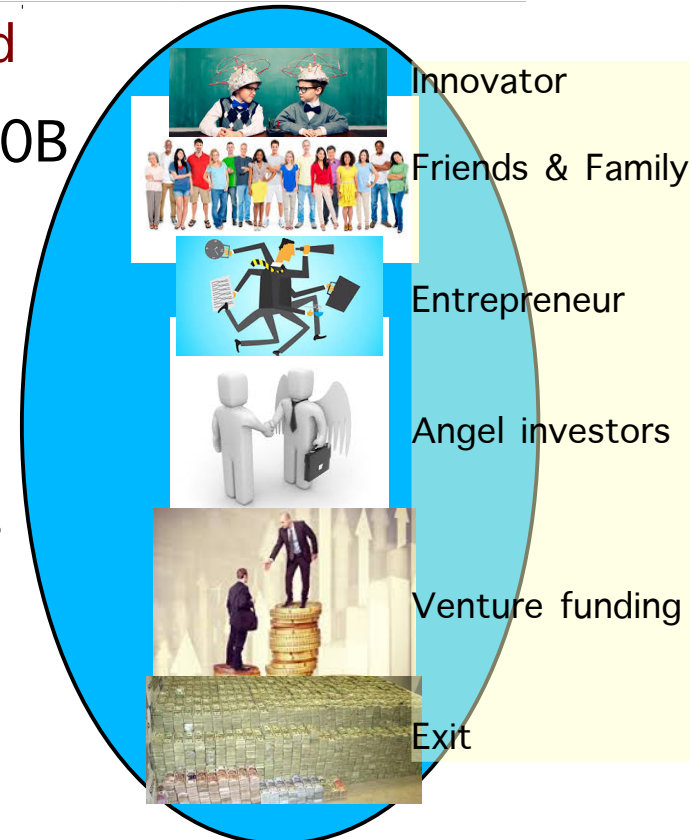
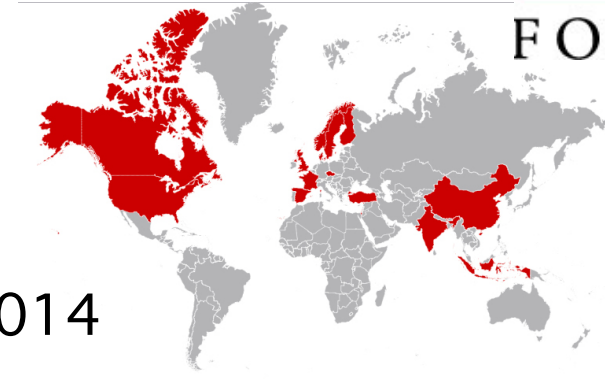
Outline

- What is “big data”?
 - How big is big?
 - Is “data” really just “data”?
- What is “cyber security”?
 - What is “cyber” about it?
 - What is “security”?
- How do they interact?
 - The who, what, where, why, when, and how of it
 - What does that mean to society?
- The past, present, and future
 - It's all about scale and business
 - Where do you want to go?



Business (and other) drivers

- Keiretsu Forum: largest private angel investment group in the World
 - 2500+ members in 46 chapters on 3 continents
 - \$80M+ invested in 125+ companies in 2015
 - ~\$750M in total investments since inception
- US: >316,00 angels funded >73,000 businesses in 2014
 - Venture backed ~4,300 businesses in the same period
- Total angel funding ~24B/y - Total venture funding ~\$50B
 - Est. 400,000 angel-backed US jobs / y
 - Many more worldwide
 - Est. 400,000 venture-backed US jobs / y
 - Most extending perviously angel-backed companies
- Pebble Beach chapter
 - I am chapter president - 1st chapter meeting in June



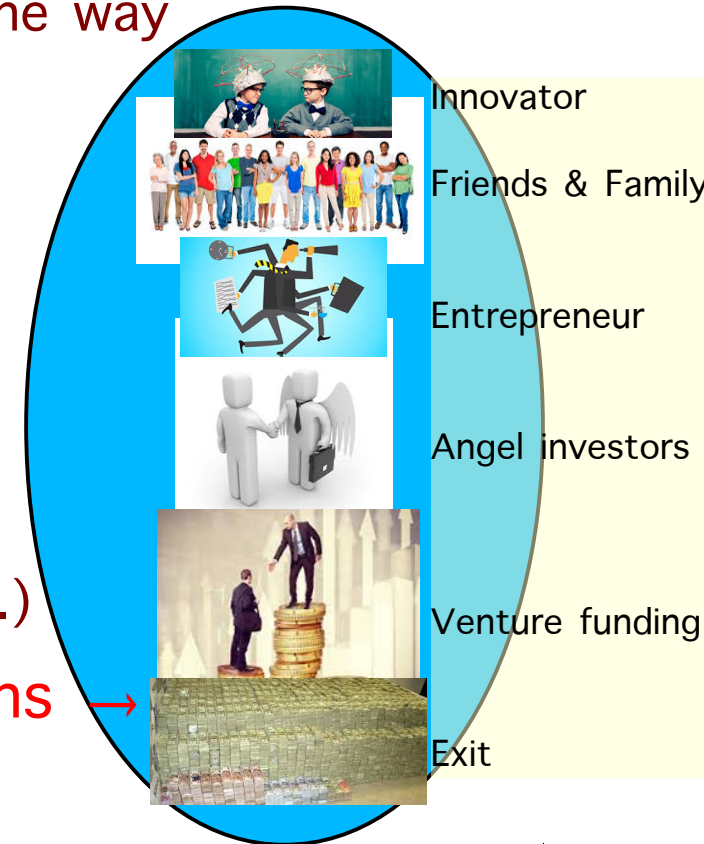
To scale it has to work for business

Big data is ... BIG!

- Size is the issue
 - Google, Amazon, Federal are big
- And getting bigger
- While the technology is getting smaller
 - Nano-scale electronics → Quantum computing
- The dynamics of the computing space is changing
 - Moore's law is about done (3d layouts, parallelism, quantum, nowhere to go)
 - Efficiency can help – for a while – but algorithms are not yet funded well
 - Energy consumption and heat dissipation are driving forces in big data today
 - A proposal for Moss Landing to cool big data by deep sea water!

There must be a path

- There must be a path from here to there
 - The path must satisfy the conditions every step of the way
 - Normal business growth likely does some of it
- Quantum, 3-d, parallel, efficiency, then what?
 - It becomes a policy (read political) issue
 - Business drivers on their own will grow till knee point
 - Someone will be willing to sell it (bigger forever)
 - Someone will be willing to buy it (power, control, etc.)
- But what of humanity? **Governments and Oligarchs** →
 - What is the ethics of big data and cyber security?
 - How far will fear drive the populace?
 - How far will engineers go?
 - If history holds ...



Will the people cow?
 Will environment win?
 What of political will?
 Will social control win?
 Security and freedom?

You've got to admit it's getting better

- By all measurable things, the human condition is improving
 - Life expectancy increasing globally
 - The poorest in the US today live better than the kings of 100 years ago
 - Less disease, pain, suffering, starvation, etc.
 - It's not that it's perfect everywhere ... it's just getting better overall
- Operational technology is bringing fabulous gains
 - Medicine is curing more diseases from OT diagnosis and treatment
 - Fewer people die in accidents when OT safety is in place
 - OT in homes, cars, planes, trains, bicycles, etc. saves lives
 - OT brings better almost everything to daily lives!
- Is cybersecurity the dark side? Or is this just FUD?:
 - The rush to market and lack of liability driving low quality into OT?
 - Low quality in OT driving vulnerabilities → opportunity for abuse → >attacks?
 - The equities issue driving offense over defense → western social collapse?

Thank You



fc at manalytic.com
Fred at KeiretsuForum.com