The Enormous Future Challenge to Systems Engineering

Artificial Intelligence, 5th Generation Communications,
and Aging, Failing Infrastructure

Mark Evans
MSEE, MS-National Resource Strategy, ASEP
President 2020, INCOSE Chesapeake Chapter
January 15, 2019

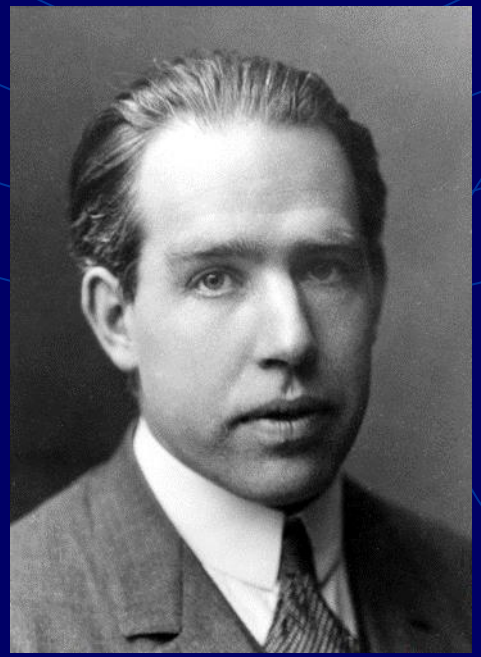
Outline

- Forecasting – a little Prediction Humor
- The 3 Existential Challenges that could "break" the SE we know & practice.
- Our definition of a Engineered System…. how it creates a boundary problem wrt. the three challenges. The challenges have no easy boundary—THAT is their greatest challenge.
- What do we do?

Forecasters BEWARE!!

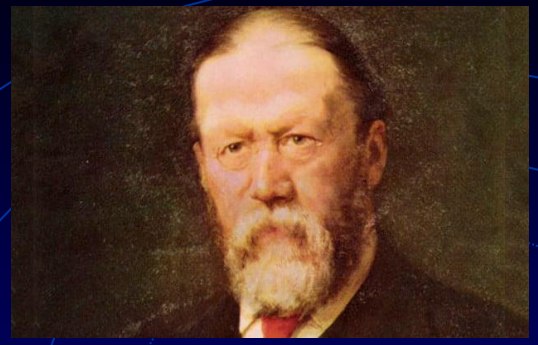
A ***WARNING*** to all Technologists and wannabe Prognosticators: there is a long list of very smart people who have tried predictions and ***FAILED***.

The people particularly bad at forecasting are CEOs, College Presidents and Presidents of companies and organizations.



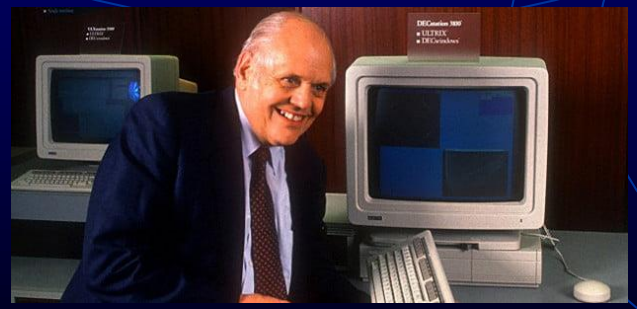
"Prediction is very difficult, especially if it is about the future."

- Niels Bohr, Nobel Prize-Physics 1922



“The Americans have need of the telephone, but we do not. We have plenty of messenger boys.”
– Sir William Preece, 1878.
William Henry Preece wasn’t uppity, nor was he a troglodyte. Preece was an electrical engineer, an inventor, an undersea telegraph cable repairman, a Morse code pioneer, the Chief Engineer of the British Post Office, and one of the earliest backers of Marconi.

“Television won’t be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night.”
– Darryl Zanuck, 20th Century Fox, 1946.



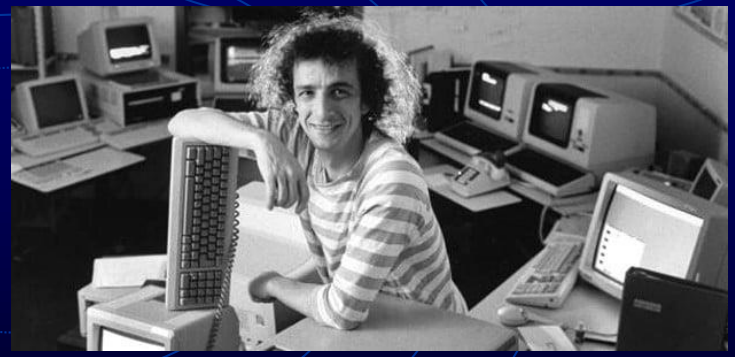
“There is no reason anyone would want a computer in their home.”
– Ken Olson, 1977
One of the all-time classic tech prediction flubs, this quote came from the lips of president, chairman and founder of Digital Equipment Corp.,

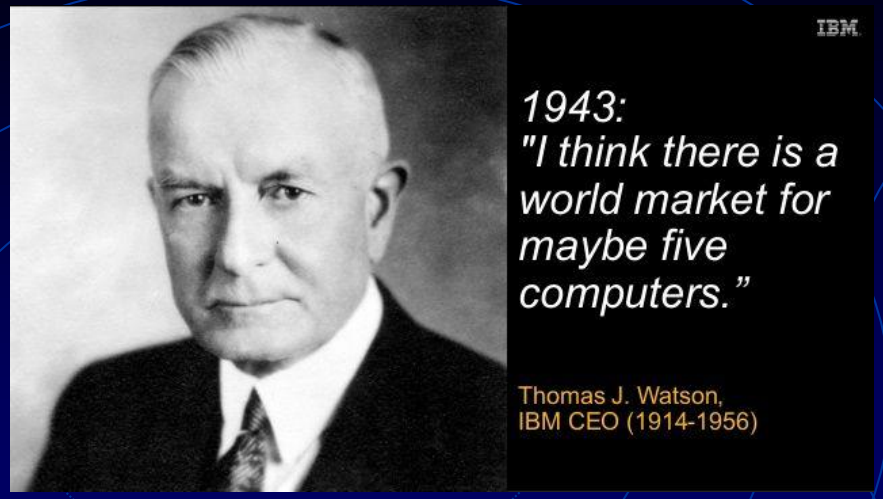
“I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse.”
– Robert Metcalfe, 1995

In 1995, Robert Metcalfe, co-invented a little thing called Ethernet and opened a little company called 3Com. The same year, in a column for InfoWorld, he famously predicted the 1996 annihilation of the Internet.

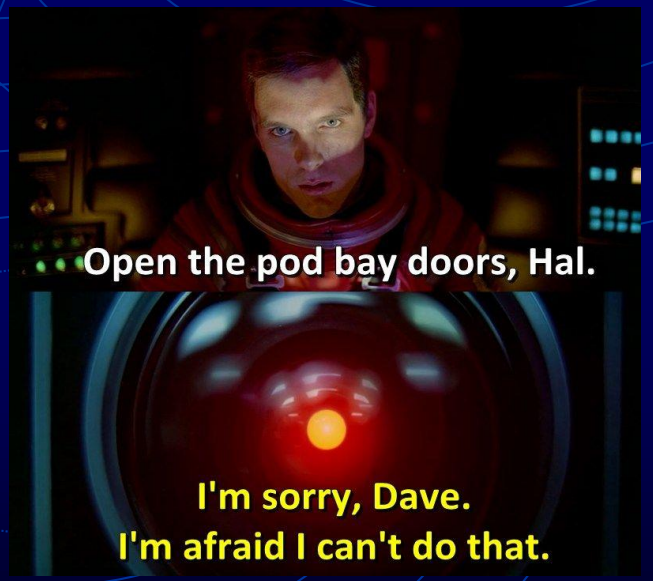
“The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.”
– Clifford Stoll, 1995

In a 1995 Newsweek column entitled “The Internet? Bah,” astronomer, author, hacker and computer geek Clifford Stoll bravely dissed the newfangled gizmo known as the WWW. He claimed it overflowed with a “cacophony” of voices and opinions – some intelligent and worthy of our attention, but many not.
He spoke of a “wasteland of unfiltered data” and problematic information searches. And he lamented there was no trustworthy way to send virtual money. Right about his present; wrong about the future.




IBM
1943:
"I think there is a world market for maybe five computers."
Thomas J. Watson,
IBM CEO (1914-1956)


640K ought to be enough for anybody
-Bill Gates, CEO Microsoft, 1981


Open the pod bay doors, Hal.
I'm sorry, Dave.
I'm afraid I can't do that.

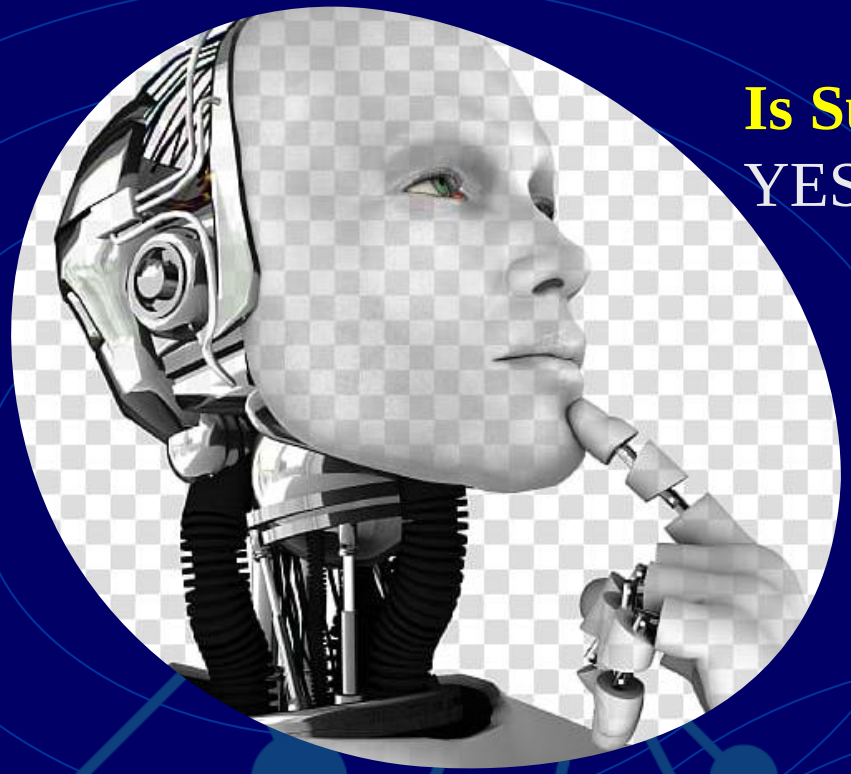
Artificial Intelligence

Intelligence = the ability to process information either naturally (carbon based) or otherwise for some reason.

Most psychologist define Intelligence as a person's ability to learn and remember information, to recognize concepts and their relations, and to apply the information to their own behavior in an adaptive way.

True AI people believe computers will eventually duplicate or surpass human capability.

The AI lament: every time AI scores big with a capability, the Engineers and CompScientists rip it out of the AI area and call it an expert system.



Is Superintelligence a real possibility?

YES, but the better question is:

What do we do before it gets here?

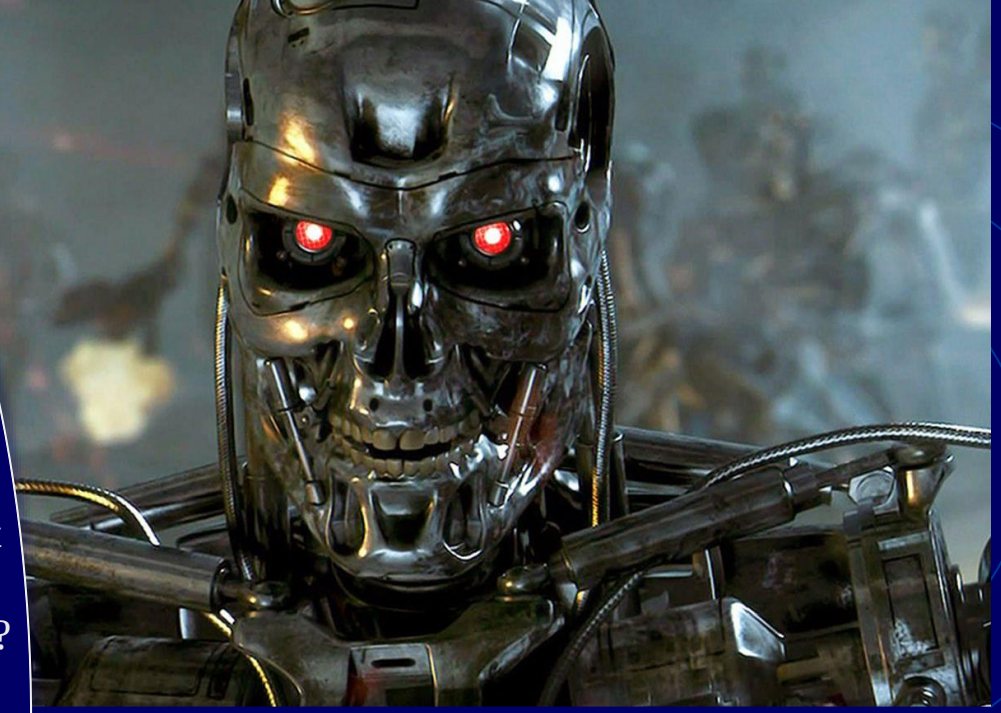
- Once an AI reaches a critical point (a singularity) the superintelligence will develop rapidly and come into existence more like an explosion

In case you missed it: AI is active and producing algorithms at an accelerating rate. The earlier well-known examples: word recognition, playing chess, solving mazes, voice recognition, automobile assembly. took years.

Recent Technical progress came faster than expected: neural Turing machines, deep reinforcement learning, Bayesian hyperparameter optimization, grid LSTMs, memory networks, variational encoders, sentence level vector embeddings, and generative adversarial networks.

The BIG Fear: Machines will take over and dominate the human species

- Robopocalyse
- Asimov's 3 Laws of Robotics are looking less like Science Fiction and more like our future bet for survival as a species
- Motivation: why would a robot race seek power? Robots are logical; not emotional, they don't have egos they are driven to satisfy.
- Would a robot species try to enslave humans to acquire more energy or more manufacturing of their machine species?
- Control: Will a robot have a survival urge? A reproductive urge? An urge to move, explore, create, design, grow?
- Need to caution against anthropomorphizing the ***capabilities*** of a superintelligent AI, as well as the ***motivations of an AI.***
- Carbon and Silicon intelligence are NOT the SAME.



Why humans may still have an edge

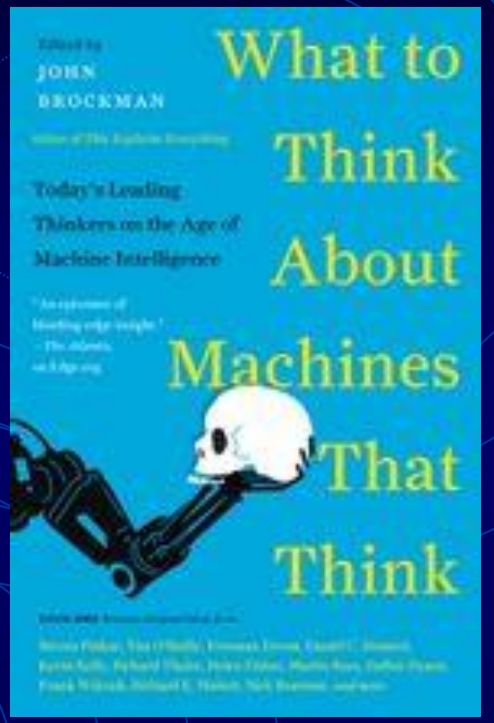
7 deadly sins— our expertise in pride, greed, lust, anger, gluttony, envy, and sloth are possibly uniquely human emotions that may not program into an artificial intelligence.

Our ability to reason; to extract ourselves from a strange or endless loop.

Godel's Incompleteness Theorem — any axiomatic system using its own rule set can construct a statement that requires going outside the system to prove ....in other words, all systems are incomplete and can be broken.... humans are very comfortable going outside of a broken system, extricating themselves from an endless loop or hopeless logic. ***This is thought to be the one advantage of humans over AI and the lower forms of natural intelligence.***

Human intelligence is resilient in the face of failure and disaster— it is this imaginative ability to envision a future not yet possible, coupled with our ability to reason that sets us apart

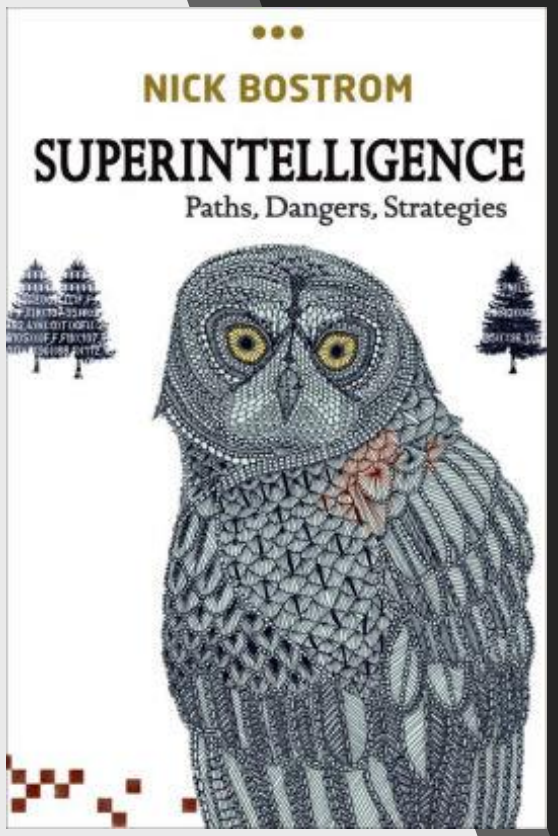
Machines need a motivation to takeover; a motivation that would have to be seeded and devolped. Evil Humans in concert with an AI is a different story.



AI gone seriously wrong

- Robopocalyse most likely won't occur by itself—someone has to teach machines the concept of evil.
- Evil Humans in the Human-Machine loop are a different story
- Adversaries may build Killer Robot Armies (AI arms race)
- Pinker points out machines don't have emotions; ability to extract themselves from strange loops or ability to reason?
- Intelligent Agents may not "want" to do mundane, menial human tasks

Coping with Super Intelligence



- When the Intelligence Explosion (singularity) gets here sometime in the 21st Century, humans will not be able to compete on a cognitive level….
- The best response: Focus Human Design Effort and Engineering on seeding the right CONTROL System….
- There are 2 broad classes for dealing with the CONTROL problem which is at the heart of AI safety: Capability control and Motivation selection.

- ***Each control method comes with potential vulnerabilities and presents different degrees of difficulty in its implementation.***

- ***The VALUE-LOADING problem or "teaching a machine to acquire values" (whatever THAT means) is one of the thorniest and still open problems for AI developments.***

Q: Does this mean SEs need to become experts in AI? A: Yes!

Control Methods for a Superintelligence

Capability Control methods	
Boxing methods	The system is confined in such a way that it can affect the external world only through some restricted, pre-approved channel. Encompasses physical and informational containment methods.
Incentive methods	The system is placed within an environment that provides appropriate incentives. This could involve social integration into a world of similarly powerful entities. Another variation is the use of (cryptographic) reward tokens. “Anthropic capture” is also a very important possibility but one that involves esoteric considerations.
Stunting	Constraints are imposed on the cognitive capabilities of the system or its ability to affect key internal processes.
Tripwires	Diagnostic tests are performed on the system (possibly without its knowledge) and a mechanism shuts down the system if dangerous activity is detected.
Motivation selection methods	
Direct specification	The system is endowed with some directly specified motivation system, which might be consequentialist or involve following a set of rules.
Domesticity	A motivation system is designed to severely limit the scope of the agent’s ambitions and activities.
Indirect normativity	Indirect normativity could involve rule-based or consequentialist principles, but is distinguished by its reliance on an indirect approach to specifying the rules that are to be followed or the values that are to be pursued.
Augmentation	One starts with a system that already has substantially human or benevolent motivations, and enhances its cognitive capacities to make it superintelligent.

The traditional approach to controlling an AI

Issac Asimov's 3 Laws of Robotics

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm;
2. A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law;
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Embarrassingly for our species, Asimov's laws remained state-of-the-art for over half a century despite obvious problems with the approach, some of which are explored in Asimov's own writings.

- Consider……how one might explain Asimov's first law to an AI.
- Does it mean that the robot should minimize the probability of any human being coming to harm? In that case the other laws become needless since it is always possible for the AI to take some action that would have at least some microscopic effect on the probability of a human being coming to harm.
- How is the robot to balance a large risk of a few humans coming to harm versus a small risk of many humans being harmed?
- How do we define "harm" anyway?
- How should the harm of physical pain be weighed against the harm of architectural ugliness or social injustice?

Superintelligence Risks and Rewards

Task	Skill set	Strategic relevance
Intelligence amplification	AI programming, cognitive enhancement research, social epistemology development, etc.	• System can bootstrap its intelligence
Strategizing	Strategic planning, forecasting, prioritizing, and analysis for optimizing chances of achieving distant goal	• Achieve distant goals • Overcome intelligent opposition
Social manipulation	Social and psychological modeling, manipulation, rhetoric persuasion	• Leverage external resources by recruiting human support • Enable a “boxed” AI to persuade its gatekeepers to let it out • Persuade states and organizations to adopt some course of action
Hacking	Finding and exploiting security flaws in computer systems	• AI can expropriate computational resources over the Internet • A boxed AI may exploit security holes to escape cybernetic confinement • Steal financial resources • Hijack infrastructure, military robots, etc.
Technology research	Design and modeling of advanced technologies (e.g. biotechnology, nanotechnology) and development paths	• Creation of powerful military force • Creation of surveillance system • Automated space colonization
Economic productivity	Various skills enabling economically productive intellectual work	• Generate wealth which can be used to buy influence, services, resources (including hardware), etc.

5th Generation Communications

The 5G promise: ***broadband access everywhere, entertaining higher user mobility, and enabling connectivity of massive number of devices (e.g. Internet of Things (IoT)) in an ultrareliable and affordable way.***

The main technological enablers : ***Cloud computing, Software Defined Networking (SDN) and Network Function Virtualization (NFV) are maturing toward 5G. However,*** ***there are pressing security challenges*** ***in these technologies and growing*** ***concerns for user privacy.***

https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions

The extreme vulnerability of 5G networks

The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. In the 5G software defined network, cyber hygiene functions are pushed outward to a web of digital routers throughout the network, and the inspection and control by hardware chokepoints is lost.

5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These standardized building block protocols and systems have proven to be valuable tools for those seeking to do ill.

The network is also being managed by software—often **early generation artificial intelligence**—that itself can be vulnerable to an attacker that gains control of the network software.

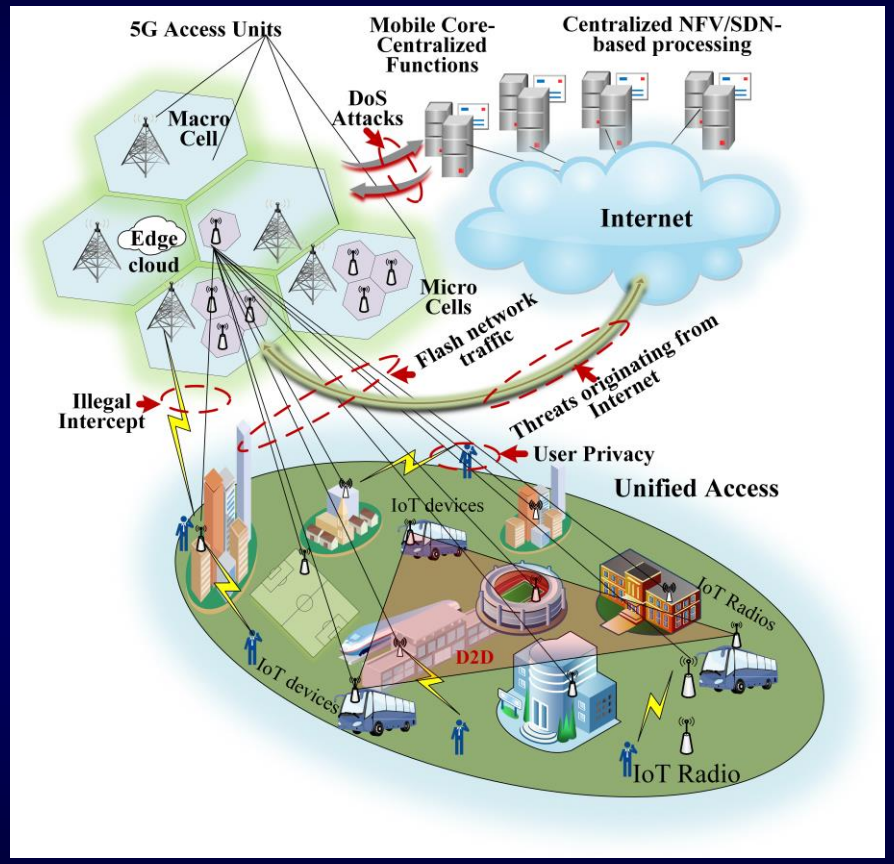
The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.

Finally, ***the vulnerability created by attaching tens of billions of hackable smart devices*** (actually, little computers) to the network colloquially referred to as **IoT.** Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, all of which are both wonderful and uniquely vulnerable.

In July, for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

Q: Does this mean SEs need to become Network & Cyber Security experts? A: Yes!

5G Security Threats and Challenges



Flash network traffic: High number of end-user devices and new things (IoT).

Security of radio interfaces: Radio interface encryption keys sent over insecure channels.

User plane integrity: No cryptographic integrity protection for the user data plane.

Mandated security in the network: Service-driven constraints on the security architecture leading to the optional use of security measures.

Roaming security: User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.

Denial of Service (DoS) attacks on the infrastructure: Visible nature of network control elements, and unencrypted control channels.

Signaling storms: Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.

DoS attacks on end-user devices: No security measures for operating systems, applications, and configuration data on user devices.

https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions

Global Interconnectivity Threats and Costs

•Malicious cyber activity **cost the U.S. economy between $57 billion and $109 billion in 2016.**

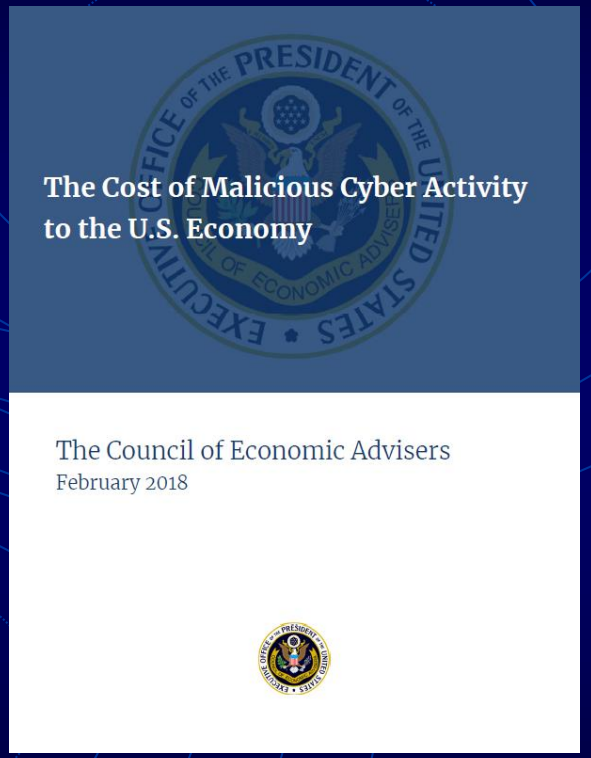
• Malicious cyber activity directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information.

• Damages from cyberattacks and cyber theft can spill over magnifying the damage to the economy.

• Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms.

• Cybersecurity is a common good; ***lax cybersecurity imposes negative externalities on other economic entities and on private citizens***. Failure to mitigate negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.

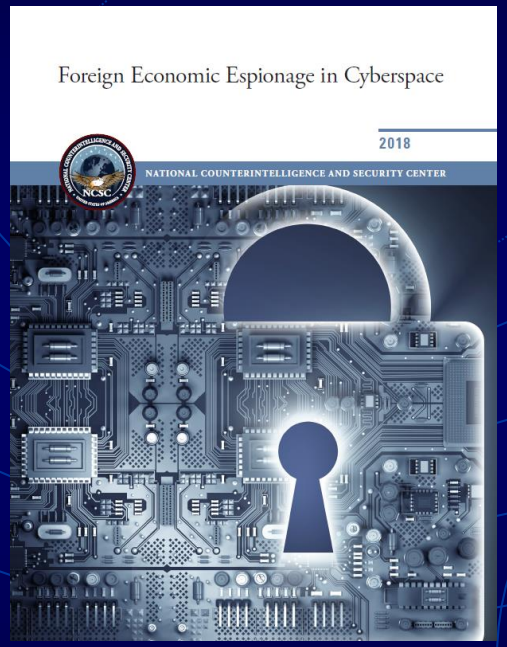
• ***Cyberattacks against critical infrastructure sectors could be highly damaging to the U.S. economy***.



• ***Bad Guys can be: Nation-states, Corporate competitors, Hacktivists, Organized criminal groups, and Company insiders.***

https://publicintelligence.net/us-malicious-cyber-activity-cost/

Foreign Economic Espionage in Cyberspace



1. In 2018, Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage.
2. Cyberspace remains a preferred operational domain.
3. **Next-generation technologies, such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared.**
4. **Building an effective response 1st requires understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade**.
5. Foreign intelligence services continue to represent the most persistent and pervasive cyber intelligence threat.
6. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and theft of U.S. information.
7. Despite advances in cybersecurity, cyber espionage continues to offer bad actors a relatively low-cost, high-yield access to a wide range of intellectual property.
8. A range of potentially disruptive threat trends warrant attention**. Software supply chain infiltration already threatens the critical infrastructure** sector and is poised to threaten other sectors.

https://publicintelligence.net/ncsc-cyber-economic-espionage/

Is there a health issue with radiation at the higher frequencies used for 5G?

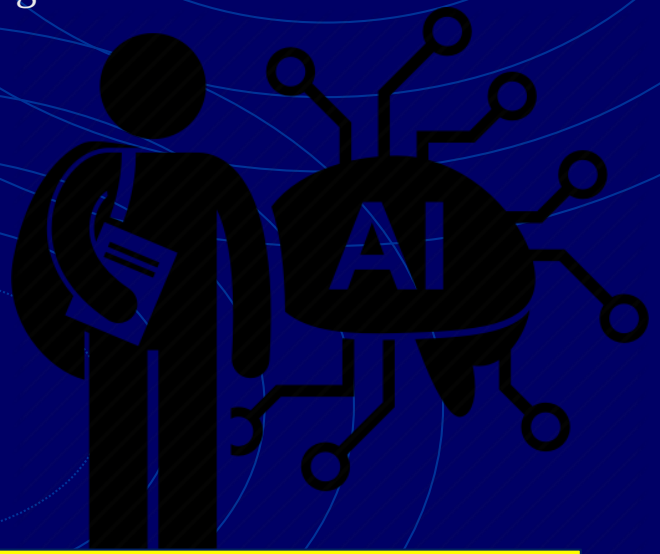
One more risk?

- It's easy to find claims online that the higher frequency of 5G constitutes a health risk.
- 1G, 2G, 3G and 4G use between 1 to 5 gigahertz. 5G uses between 24 to 90 gigahertz. There are several assertions about the RF Radiation portion of the electromagnetic spectrum, the higher the frequency, the more dangerous it is to living organisms."
- But asserting that the higher frequency is more dangerous is just that—an assertion, and there's little real science to stand behind it.
- 5G remains non-ionizing in nature.

https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/

Addressing Cyber Security

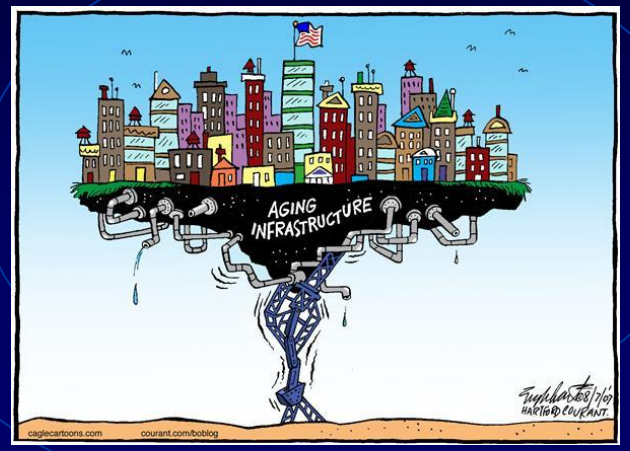
- INCOSE 2025: Systems engineering routinely incorporates requirements to enhance systems and information security and resiliency to cyber threats early and is able to verify the cyber defense capabilities over the full system life cycle, based on an increasing body of strategies, tools and methods.
- Cyber security is a fundamental system attribute that systems engineers understand and incorporate into designs using the following strategies:



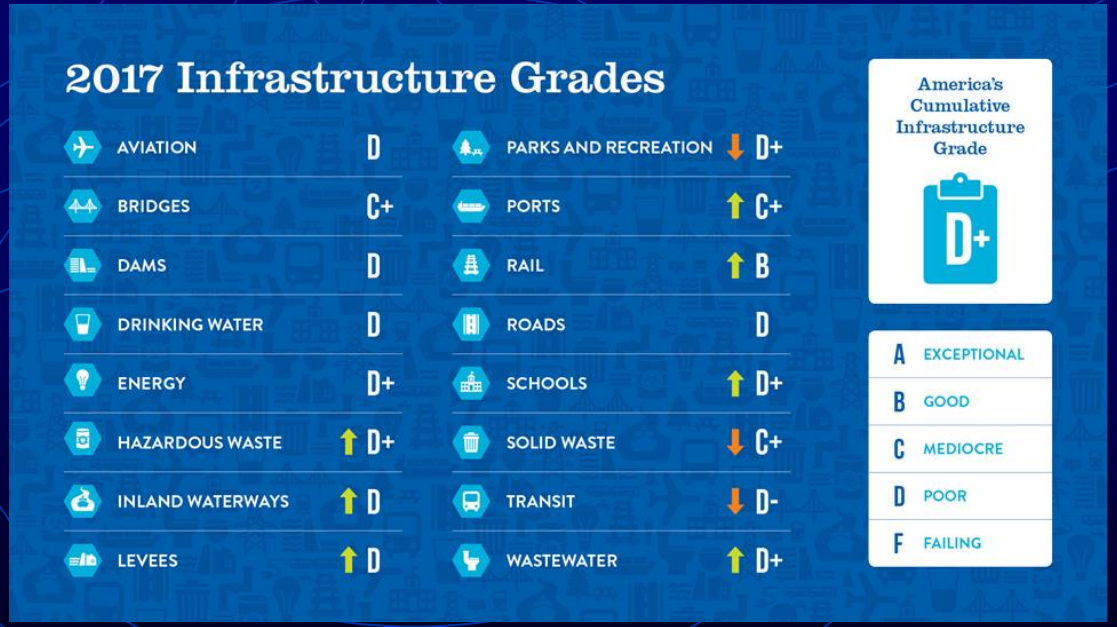
- Continuous threat and system behavior monitoring
- Management of access rights and privileges
- Use of testbeds for assessing new threats in fielded systems
- Supply-chain diligence
- Certification and accreditation standards
- Formal methods for identification of vulnerabilities

The INCOSE Vision recognizes that Cyber Security has become another key skill the SE must have a working knowledge of.

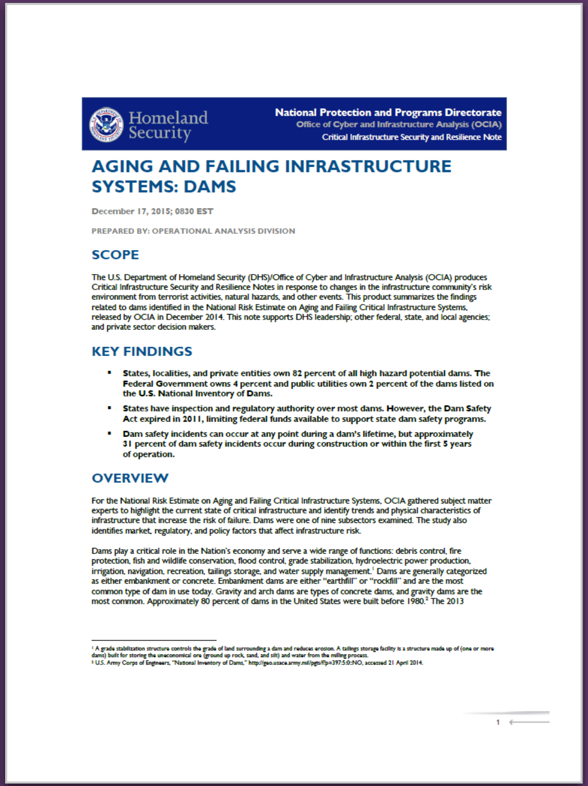
The Aging Infrastructure



- Every 4 years, the ASCE Foundation grades the US Infrastructure.
- The *2017 Infrastructure Report Card* reveals that we have made some incremental progress toward restoring our nation's infrastructure.
- But it has not been enough. As in 2013, ***America's cumulative GPA is once again a D+.***



https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/Grades-Chart.png



Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

AGING AND FAILING INFRASTRUCTURE SYSTEMS: DAMS

December 17, 2015; 0830 EST

PREPARED BY: OPERATIONAL ANALYSIS DIVISION

SCOPE

The U.S. Department of Homeland Security (DHS)/Office of Cyber and Infrastructure Analysis (OCIA) produces Critical Infrastructure Security and Resilience Notes in response to changes in the infrastructure community's risk environment from terrorist activities, natural hazards, and other events. This product summarizes the findings related to dams identified in the National Risk Estimate on Aging and Failing Critical Infrastructure Systems, released by OCIA in December 2014. This note supports DHS leadership; other federal, state, and local agencies; and private sector decision makers.

KEY FINDINGS

- **States, localities, and private entities own 82 percent of all high hazard potential dams. The Federal Government owns 4 percent and public utilities own 2 percent of the dams listed on the U.S. National Inventory of Dams.**
- **States have inspection and regulatory authority over most dams. However, the Dam Safety Act expired in 2011, limiting federal funds available to support state dam safety programs.**
- **Dam safety incidents can occur at any point during a dam's lifetime, but approximately 31 percent of dam safety incidents occur during construction or within the first 5 years of operation.**

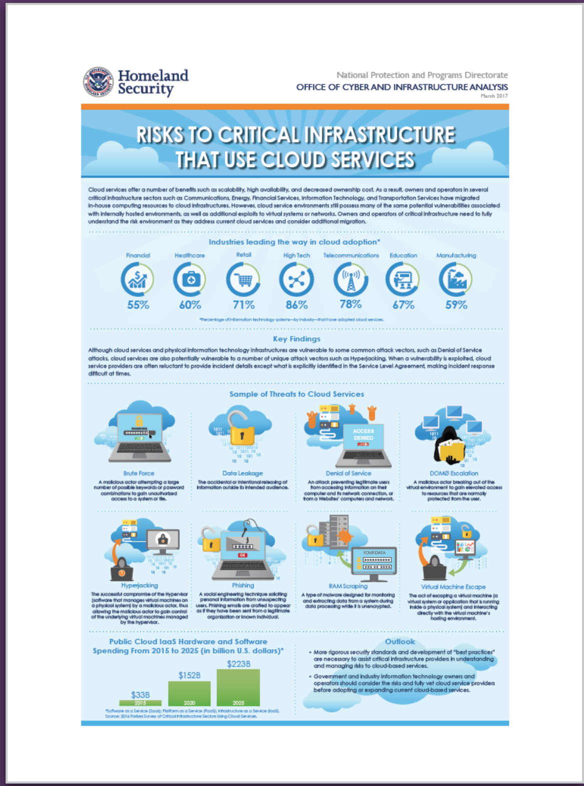
OVERVIEW

For the National Risk Estimate on Aging and Failing Critical Infrastructure Systems, OCIA gathered subject matter experts to highlight the current state of critical infrastructure and identify trends and physical characteristics of infrastructure that increase the risk of failure. Dams were one of nine subsectors examined. The study also identifies market, regulatory, and policy factors that affect infrastructure risk.

Dams play a critical role in the Nation's economy and serve a wide range of functions: debris control, fire protection, fish and wildlife conservation, flood control, grade stabilization, hydroelectric power production, irrigation, navigation, recreation, tailings storage, and water supply management.[1] Dams are generally categorized as either embankment or concrete. Embankment dams are either "earthfill" or "rockfill" and are the most common type of dam in use today. Gravity and arch dams are types of concrete dams, and gravity dams are the most common. Approximately 80 percent of dams in the United States were built before 1980.[2] The 2013

[1] A grade stabilization structure controls the grade of land surrounding a dam and reduces erosion. A tailings storage facility is a structure made up of (one or more dams) built for storing the uneconomical ore (ground up rock, sand, and silt) and water from the milling process.
[2] U.S. Army Corps of Engineers, "National Inventory of Dams," http://geo.usace.army.mil/pgis/f?p=397:5:0::NO, accessed 21 April 2014.

1



Homeland Security

National Protection and Programs Directorate
OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS
March 2017

RISKS TO CRITICAL INFRASTRUCTURE THAT USE CLOUD SERVICES

Cloud services offer a number of benefits such as scalability, high availability, and decreased ownership cost. As a result, owners and operators in several critical infrastructure sectors such as Communications, Energy, Financial Services, Information Technology, and Transportation Services have migrated in-house computing resources to cloud infrastructures. However, cloud service environments still possess many of the same potential vulnerabilities associated with internally hosted environments, as well as additional exploits to virtual systems or networks. Owners and operators of critical infrastructure need to fully understand the risk environment as they address current cloud services and consider additional migration.

Key Findings

Although cloud services and physical information technology infrastructures are vulnerable to some common attack vectors, such as Denial of Service attacks, cloud services are also potentially vulnerable to a number of unique attack vectors such as Hyperjacking. When a vulnerability is exploited, cloud service providers are often reluctant to provide incident details except what is explicitly identified in the Service Level Agreement, making incident response difficult at times.

Sample of Threats to Cloud Services

Brute Force: A malicious actor attempting a large number of possible keywords or password combinations to gain unauthorized access to a system or file.

Data Leakage: The accidental or intentional releasing of information outside its intended audience.

Denial of Service: An attack preventing legitimate users from accessing information on their computer and its network connection, or from a Websites' computers and network.

DOMØ Escalation: A malicious actor breaking out of the virtual environment to gain elevated access to resources that are normally protected from the user.

Hyperjacking: The successful compromise of the Hypervisor (software that manages virtual machines on a physical system) by a malicious actor, thus allowing the malicious actor to gain control of the underlying virtual machines managed by the hypervisor.

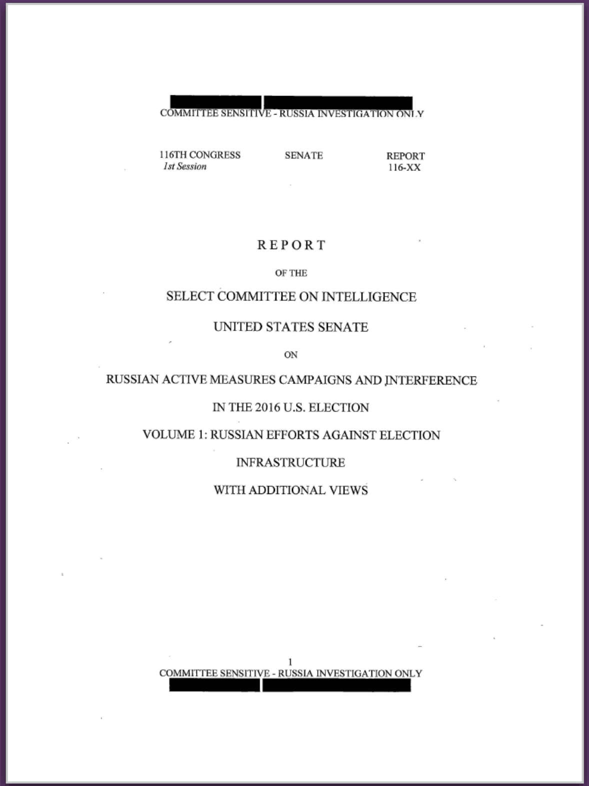
Phishing: A social engineering technique soliciting personal information from unsuspecting users. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual.

RAM Scraping: A type of malware designed for monitoring and extracting data from a system during data processing while it is unencrypted.

Virtual Machine Escape: The act of escaping a virtual machine (a virtual system or application that is running inside a physical system) and interacting directly with the virtual machine's hosting environment.

Outlook

- More rigorous security standards and development of "best practices" are necessary to assist critical infrastructure providers in understanding and managing risks to cloud-based services.
- Government and industry information technology owners and operators should consider the risks and fully vet cloud service providers before adopting or expanding current cloud-based services.



[redacted]
COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

116TH CONGRESS
1st Session

SENATE

REPORT
116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE

IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION

INFRASTRUCTURE

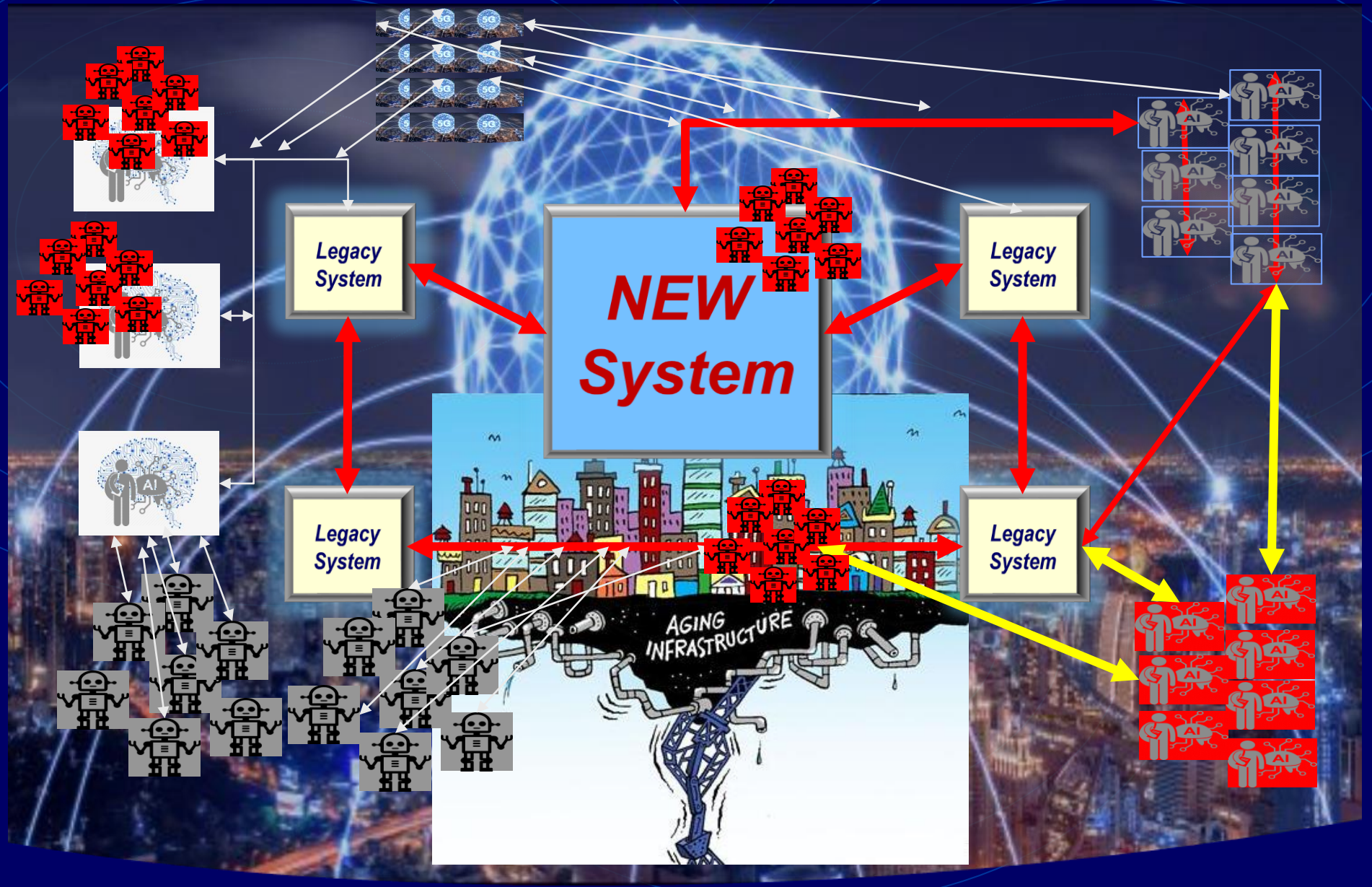
WITH ADDITIONAL VIEWS

1

COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY
[redacted]

Critical Risks to US Infrastructure

The FUTURE System Environment… is here NOW!



The FUTURE System Environment… is here NOW!

WHAT do we DO?

- Read, Research, Reflect, Revisit, Relearn, Redesign, Revise, Retrofit, Retest, Adapt, Repeat; …..
- Try to incorporate methods from other disciplines

VIRTUAL ENGINEERING

Simulation and Visualization

Modeling, simulation, and visualization enable complex system understanding that help us anticipate and verify solutions and their cost before building them. As systems become more complex, understanding their emergent behavior due to increasingly complex software, extreme physical environments, net-centricity, and human interactions becomes essential for successful systems development.

Modeling, simulation and visualization will become more integrated and powerful to cope with the systems challenges in 2025.

Integrated Model-based Approaches

Model-based Systems Engineering will become the "norm" for systems engineering execution, with specific focus placed on integrated modeling environments. These systems models go "beyond the boxes", incorporating geometric, production and operational views. Integrated models reduce inconsistencies, enable automation and support early and continual verification by analysis.

DARPA's Adaptive Vehicle Make program is setting the vision for the future of an integrated, model-based tool chain.

Transforming Virtual Model to Reality

A shift towards an integrated, digital engineering environment enables rapid transformation of concepts and designs to physical prototypes through the application of additive manufacturing technologies, such as 3D printers. This capability enables engineers to rapidly and continually assess and update their designs prior to committing costs to production hardware. The Boeing 777 virtual design process establishes a point of departure for the future of highly integrated, virtual design and production. Systems engineering practices will leverage this capability to rapidly assess alternative designs in terms of their form, fit and function.

Digital printing and related technologies enable rapid iterations from concept to hardware prototype and even production.

What do we do?

INCOSE 2025 has a vision for the future with a particular emphasis upon MBSE

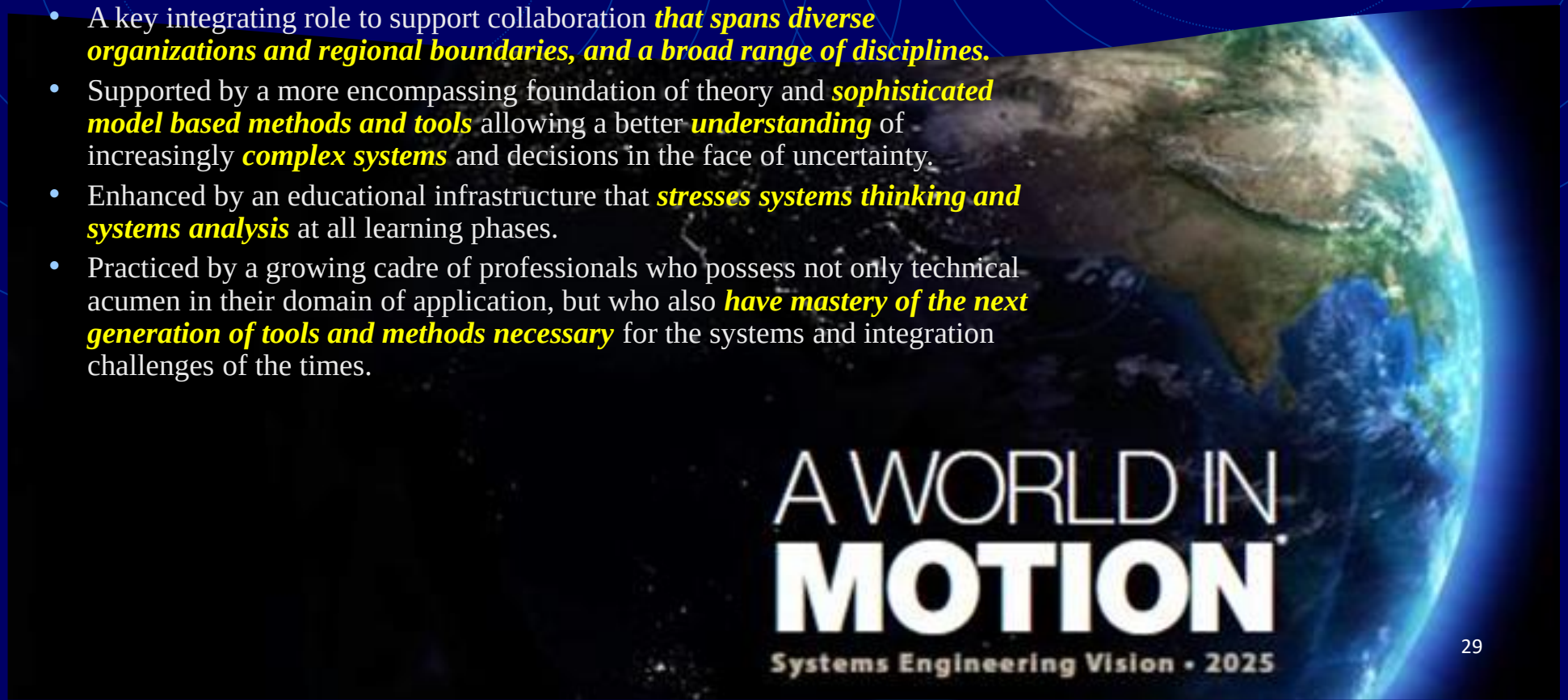
SE Vision 2025 addresses the AI threat generally, the 5G threat specifically, and infrastructures generally

Several of our colleagues are already out-front leading with solutions described in important papers

Systems Engineering will be….

INCOSE
2025 Vision

- ***Relevant to a broad range of application domains***, well beyond its traditional roots in aerospace and defense, to meet society's growing quest for sustainable system solutions to providing fundamental needs, in the globally competitive environment.
- ***Applied more widely to assessments*** of socio-physical systems in support of policy decisions and other forms of remediation.
- Comprehensively ***integrating multiple market, social and environmental*** stakeholder demands against "end to end" life cycle considerations and long term risks.
- A key integrating role to support collaboration ***that spans diverse organizations and regional boundaries, and a broad range of disciplines.***
- Supported by a more encompassing foundation of theory and ***sophisticated model based methods and tools*** allowing a better ***understanding*** of increasingly ***complex systems*** and decisions in the face of uncertainty.
- Enhanced by an educational infrastructure that ***stresses systems thinking and systems analysis*** at all learning phases.
- Practiced by a growing cadre of professionals who possess not only technical acumen in their domain of application, but who also ***have mastery of the next generation of tools and methods necessary*** for the systems and integration challenges of the times.

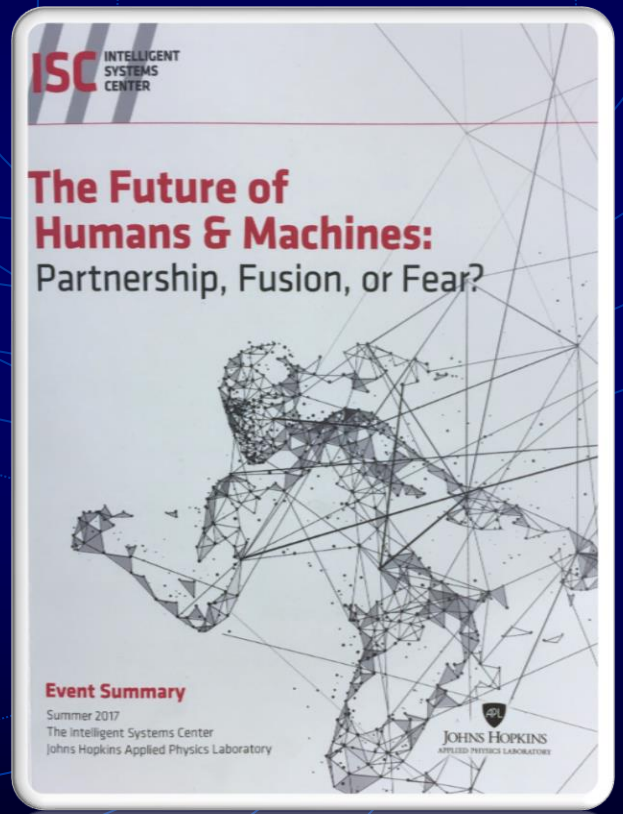


Addressing the AI Challenge

Technical Conferences set the tone and direction

Conclusions from the JHU/APL May 25, 2017 Conference on AI:

- While sentient machines are likely a long way off, the opportunities and risks posed by complex autonomous systems are here today.
- Intelligent machines are changing the nature of war.
- Machines don't know what they don't know (and neither do we).
- For the foreseeable future, teams of humans and machines will be more effective than either working alone.
- Emerging brain interfaces may enable thought-based communication and control between humans and machines in the near future (without brain surgery)
- In Artificial Intelligence, humanity has created our most sophisticated set of tools yet, with potential that may even reach what we've imagined in science fiction.



Linear Systems Theory

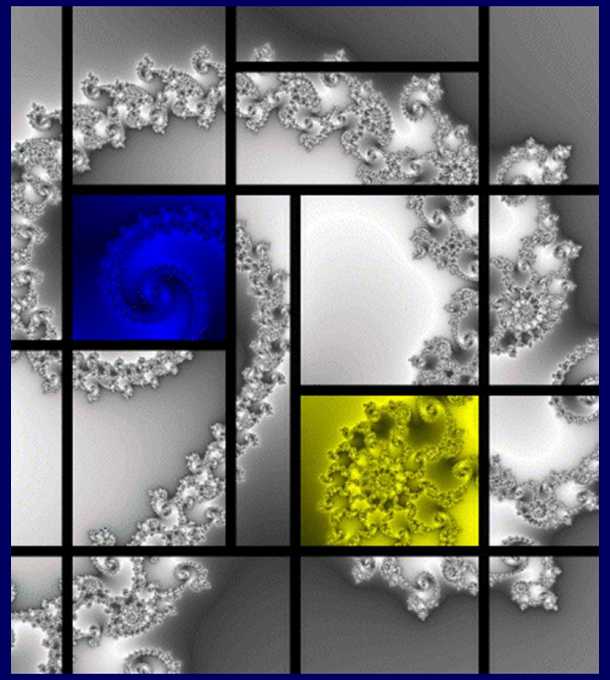
Most of our Systems Developments use Linear Mathematics

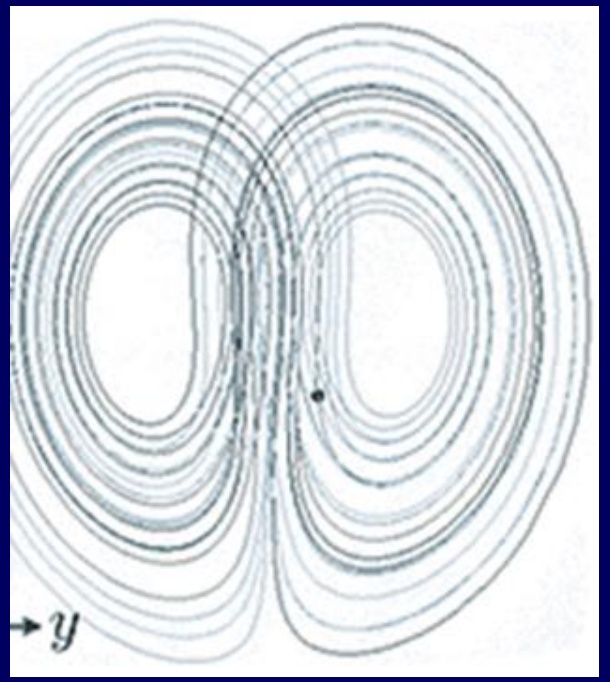
- ***Quick Review: Linear Systems***
- Homogeneity (Scaling)
- Additivity
- Together:

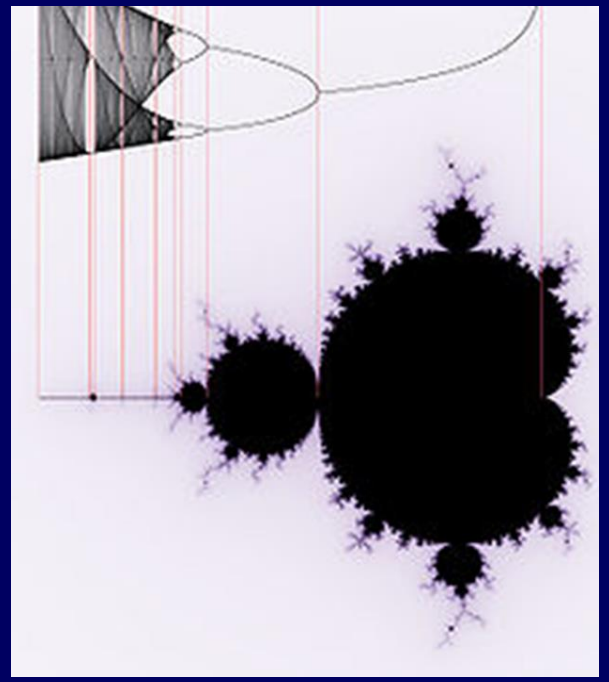
  Homogeneity AND Additivity= Principle of SUPERPOSITION
- Shift-Invariance

https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html

- **Why we use Linear Math to describe Systems:**
- **Simpler**
- Characterizing the complete input-output properties of a system by exhaustive measurement is usually impossible.
- When a system qualifies as a *linear system*, it is possible to use the responses to a small set of inputs to predict the response to any possible input.
- This can save the scientist/engineer enormous amounts of work, and *makes it possible to characterize the system completely*.







Non-linear Systems are:

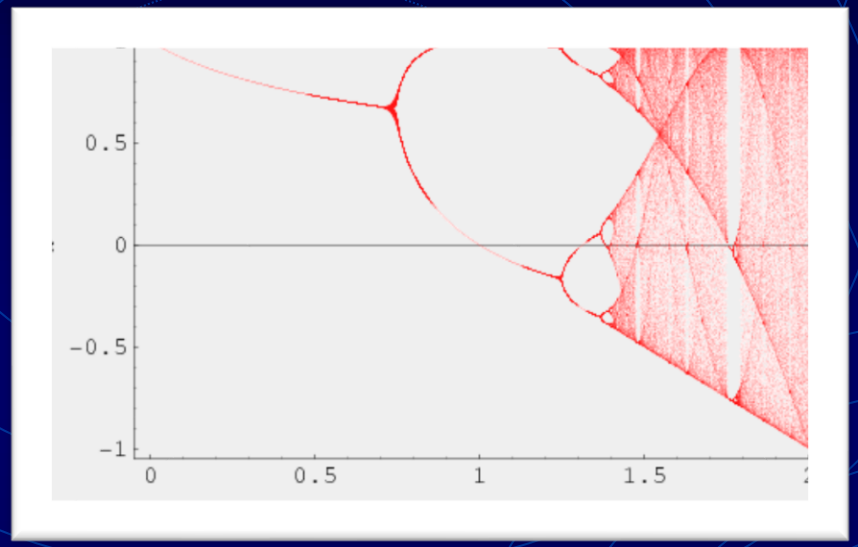
- Messy Mathematics.
- Hard to model…..
- Produce outputs that are frequently non-repeatable.
- Everything linear systems are not….
- Real world….

Mitchell Feigenbaum

- Born in New York City, to Polish and Ukrainian Jewish immigrants.
- Attended Samuel J. Tilden High School, in Brooklyn, and City College of New York.
- Graduate studies at the Massachusetts Institute of Technology (MIT) in electrical engineering and then changed to physics. (1964)
- Cornell University (1970–1972)
- Virginia Polytechnic Institute and State University (1972–1974)
- Long term post at the Los Alamos National Laboratory in New Mexico to study turbulence in fluids. His research led to a study of chaotic maps.[2]
- 1986, awarded the Wolf Prize in Physics "for his pioneering theoretical studies demonstrating the universal character of non-linear systems, which has made possible the systematic study of chaos".
- ***Discovered the Universality Principle buried deep within Dynamical Systems and Chaos***

The Feigenbaum Constant

A Monumental Achievement that launched a new science



Feigenbaum Diagram of the iterated function

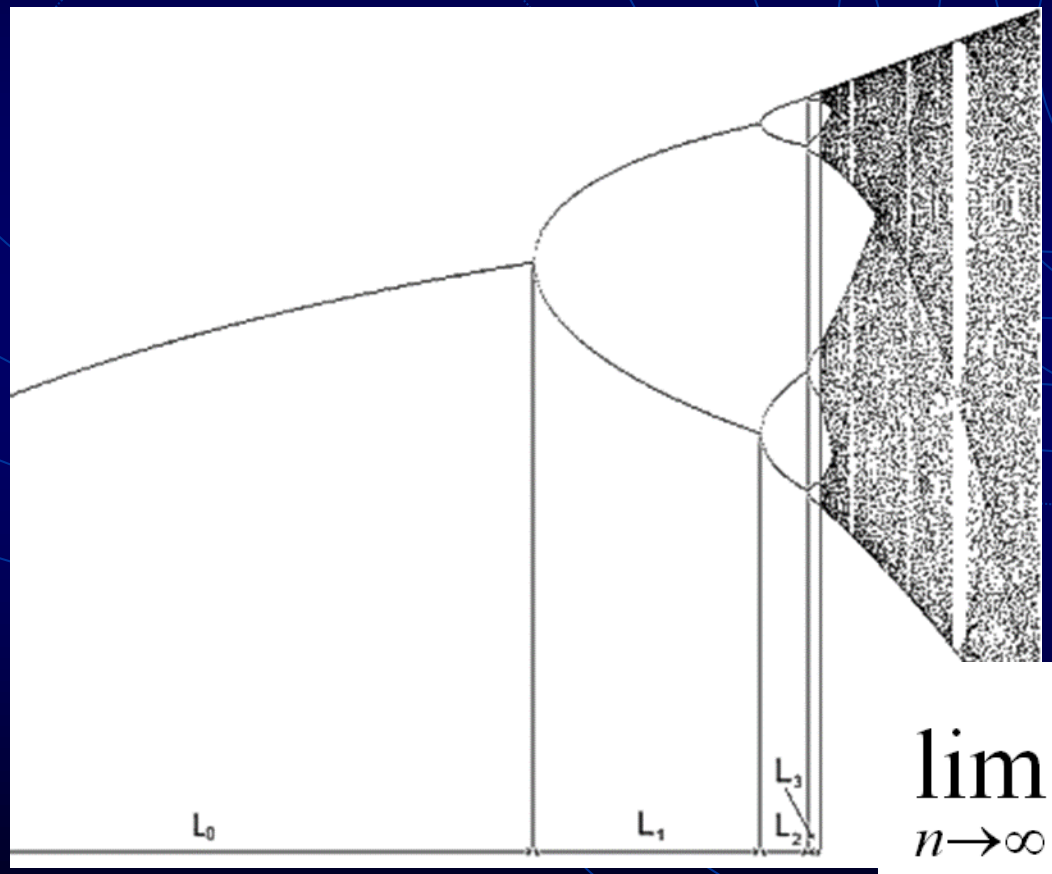
$$f(x) = 1 - \mu|x|^r$$

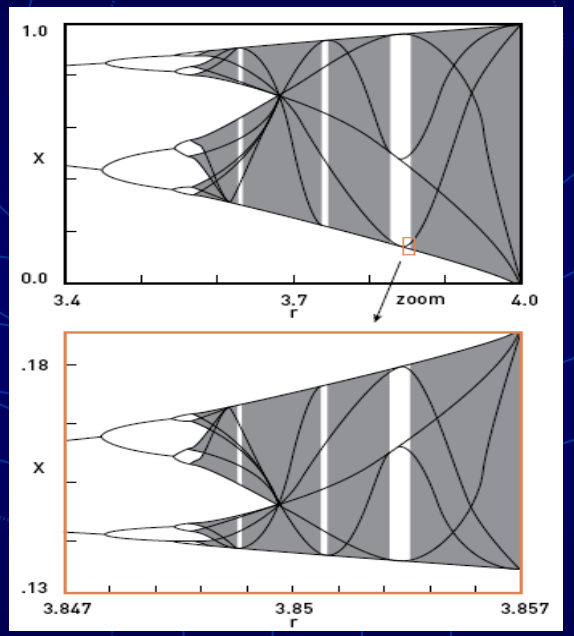
"The number $\delta = 4.6692\ldots$ is a constant of chaos comparable only to the fundamental importance of numbers like π. Feigenbaum's discovery was the first of many footprints by which the tracks of chaos are now recognized. It has been documented in systems as diverse as dripping faucets, oscillations of liquid helium, and gypsy moth population variances."

Chaos and Fractals, 1992,p.590

The Feigenbaum Constant

Discovery of ***Universality*** within Chaos





$$\lim_{n\to\infty} \frac{r_n - r_{n-1}}{r_{n+1} - r_n} = 4.669\ldots$$

https://commons.wikimedia.org/w/index.php?curid=1250389

We need to use ***Different Mathematics***

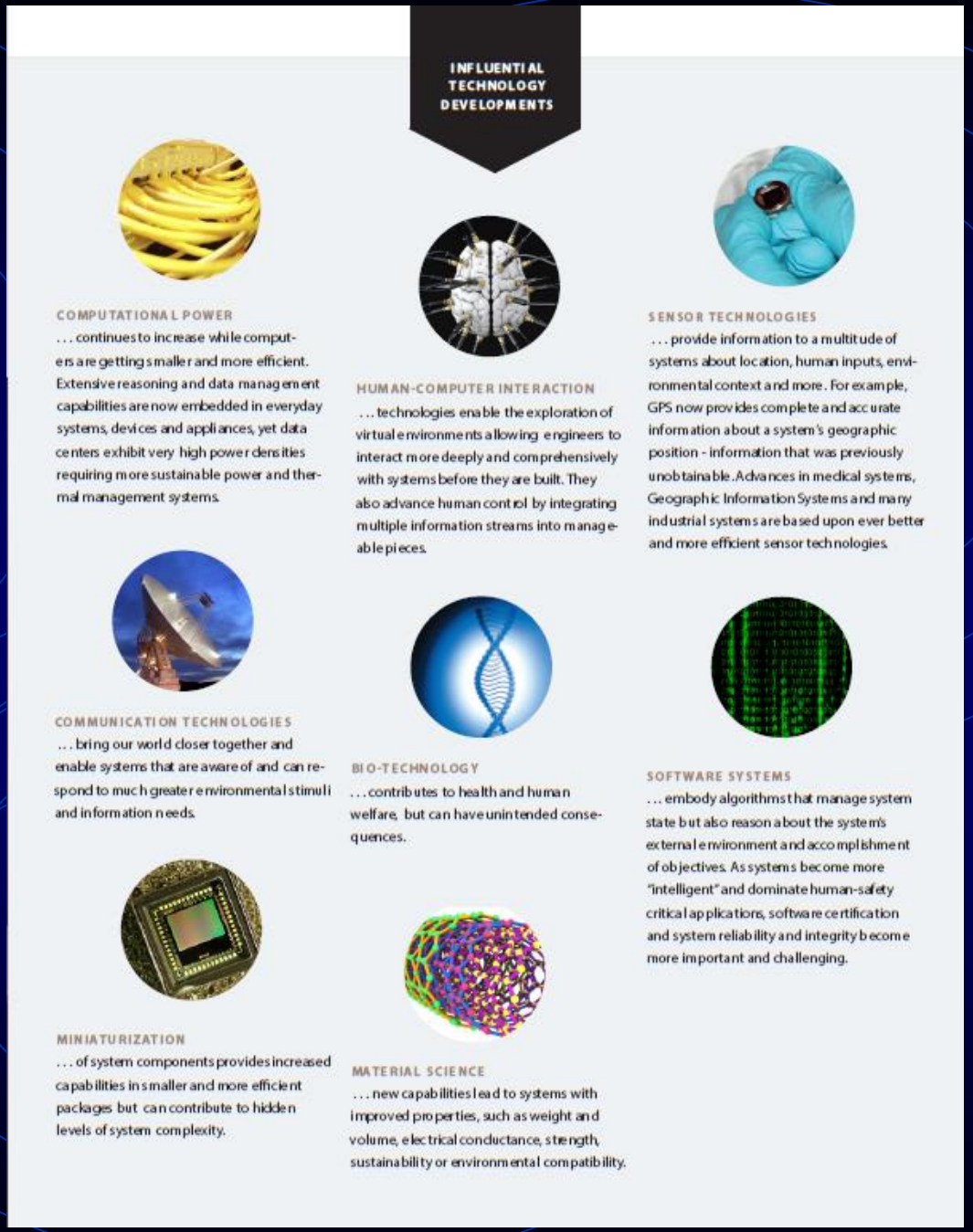
- The real world is non-linear
- SE and MBSE use linear, Gaussian mathematics for engineering systems because it simplifies the problem, and the mathematics are more manageable (doable)
- A Complexity Primer for Systems Engineers INCOSE (2015 Whitepaper) advocates some non-linear analytic techniques

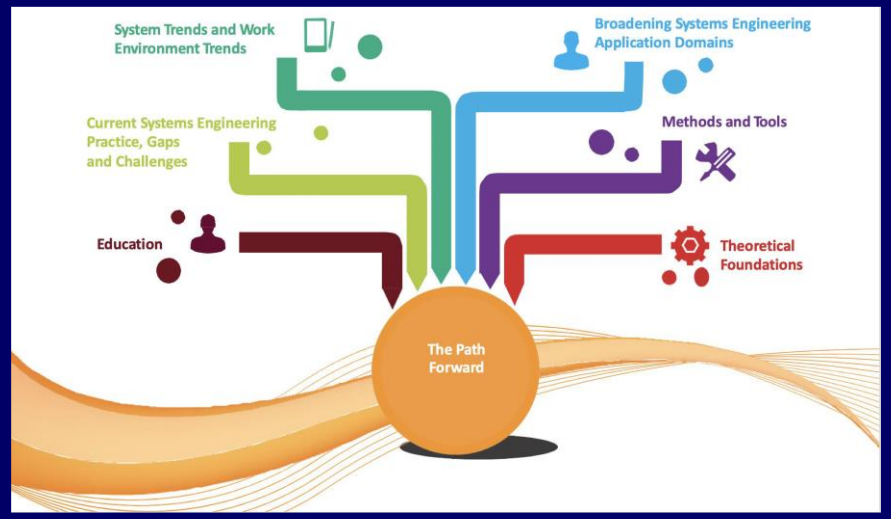
Table 3. Selected modeling methods for complex systems from the Cook Matrix.

ANALYZE	DIAGNOSE	MODEL	SYNTHESIZE
Data Mining	Algorithmic Complexity	Uncertainty Modeling	Design Structure Matrix
Splines	Monte Carlo Methods	Virtual Immersive Modeling	Architectural Frameworks
Fuzzy Logic	Thermodynamic Depth	Functional / Behavioral Models	Simulated Annealing
Neural Networks	Fractal Dimension	Feedback Control Models	Artificial Immune System
Classification & Regression Trees	Information Theory	Dissipative Systems	Particle Swarm Optimization
Kernel Machines	Statistical Complexity	Game Theory	Genetic Algorithms
Nonlinear Time Series Analysis	Graph Theory	Cellular Automata	Multi-Agent Systems
Markov Chains	Functional Information	System Dynamics	Adaptive Networks
Power Law Statistics	Multi-scale Complexity	Dynamical Systems	
Social Network Analysis		Network Models	
		Agent Based Models	
		Multi-Scale Models	

SE Vision 2025

- Technological advances in basic components, sub-systems and infrastructure will produce innovations at an increasing pace, leading to sophisticated new services and products.
- The internet, for example, has progressed from an emerging technology to having a profound impact on commerce and our personal lives in just 20 years.
- These new services and products will both depend upon and result in new, evermore complex systems.
- With technology infusion rates increasing, the pressure of time to market will also increase, yet customers will be expecting improved product functionality, aesthetics, operability, and overall value.



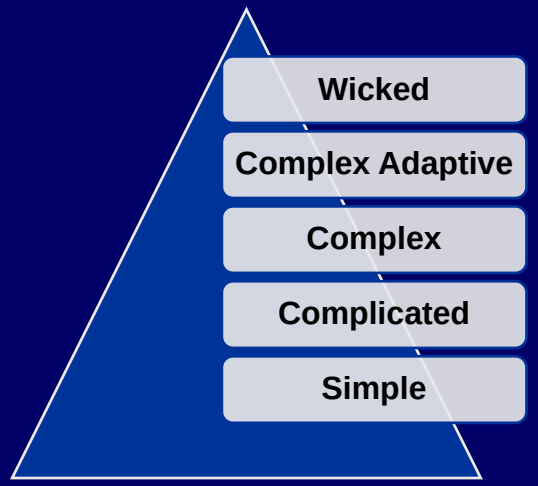


SE Vision 2025

- Addresses the 3 threats Generally
- The Path Forward is very specific about :
  Model-based SE becoming the primary method
- Cross-discipline knowledge and techniques being used by all SEs

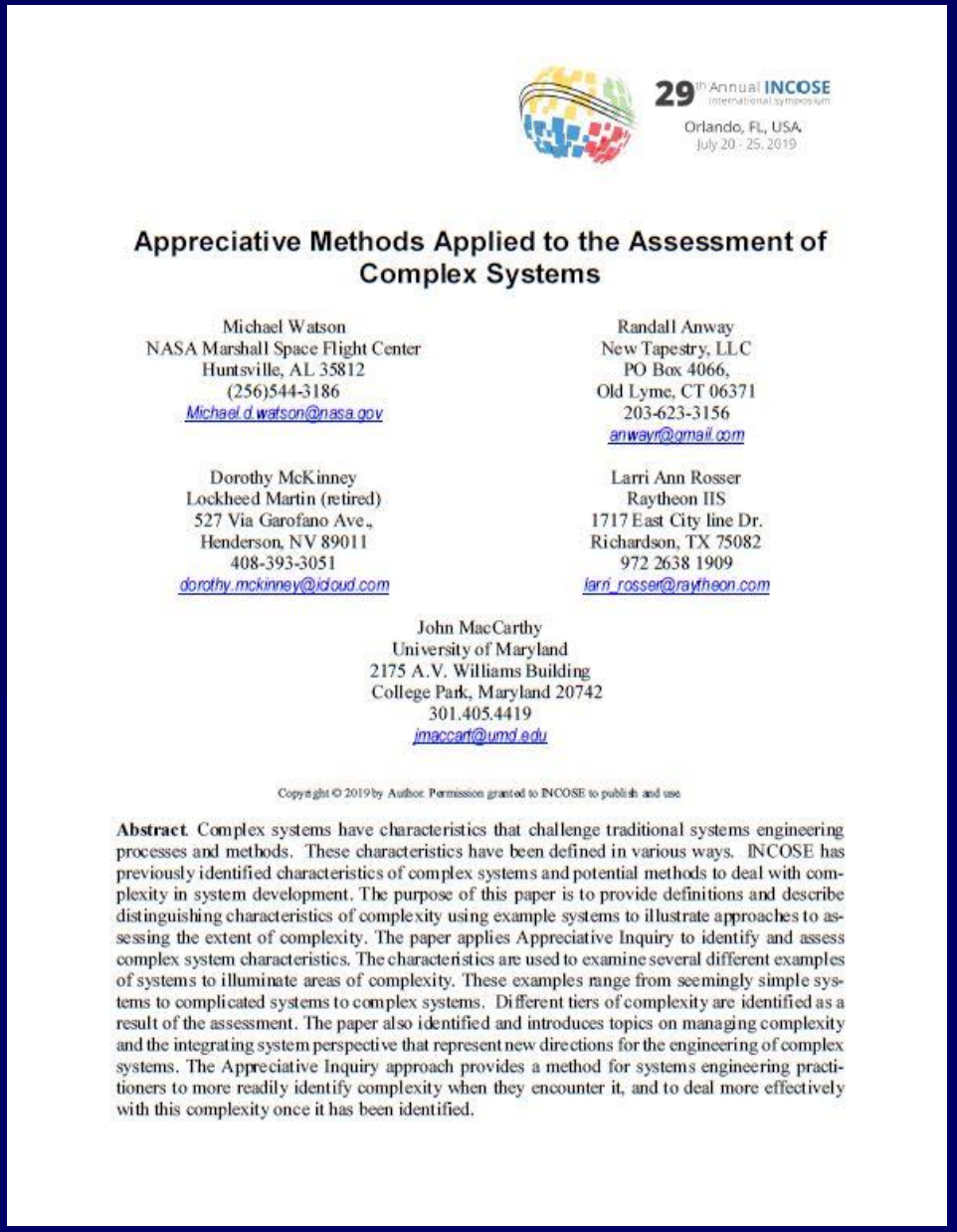
The Hierarchy of Complexity

- Where an engineering problem set resides on this complexity tier structure has everything to do with the method used to approach the problem
- Systems Engineers must learn new methods to address top 2 problem classes: “Wicked” and Complex Adaptive



Assessment of Complex Systems

- Difficult to Do
- Still in its infancy
- Non-Linear Methods using AI is necessary to engineer the complex system.
- The time and effort to fully model a complex system typically exceeds the schedule and budgetary resources of the project. Behavior is nonlinear which means extrapolation of current conditions leads to errors in understanding.



29th Annual INCOSE international symposium
Orlando, FL, USA
July 20 - 25, 2019

Appreciative Methods Applied to the Assessment of Complex Systems

Michael Watson
NASA Marshall Space Flight Center
Huntsville, AL 35812
(256)544-3186
Michael.d.watson@nasa.gov

Randall Anway
New Tapestry, LLC
PO Box 4066,
Old Lyme, CT 06371
203-623-3156
anwayr@gmail.com

Dorothy McKinney
Lockheed Martin (retired)
527 Via Garofano Ave.,
Henderson, NV 89011
408-393-3051
dorothy.mckinney@icloud.com

Larri Ann Rosser
Raytheon IIS
1717 East City line Dr.
Richardson, TX 75082
972 2638 1909
larri_rosser@raytheon.com

John MacCarthy
University of Maryland
2175 A.V. Williams Building
College Park, Maryland 20742
301.405.4419
jmaccart@umd.edu

Abstract. Complex systems have characteristics that challenge traditional systems engineering processes and methods. These characteristics have been defined in various ways. INCOSE has previously identified characteristics of complex systems and potential methods to deal with complexity in system development. The purpose of this paper is to provide definitions and describe distinguishing characteristics of complexity using example systems to illustrate approaches to assessing the extent of complexity. The paper applies Appreciative Inquiry to identify and assess complex system characteristics. The characteristics are used to examine several different examples of systems to illuminate areas of complexity. These examples range from seemingly simple systems to complicated systems to complex systems. Different tiers of complexity are identified as a result of the assessment. The paper also identified and introduces topics on managing complexity and the integrating system perspective that represent new directions for the engineering of complex systems. The Appreciative Inquiry approach provides a method for systems engineering practitioners to more readily identify complexity when they encounter it, and to deal more effectively with this complexity once it has been identified.

The General Nature of System Complexity

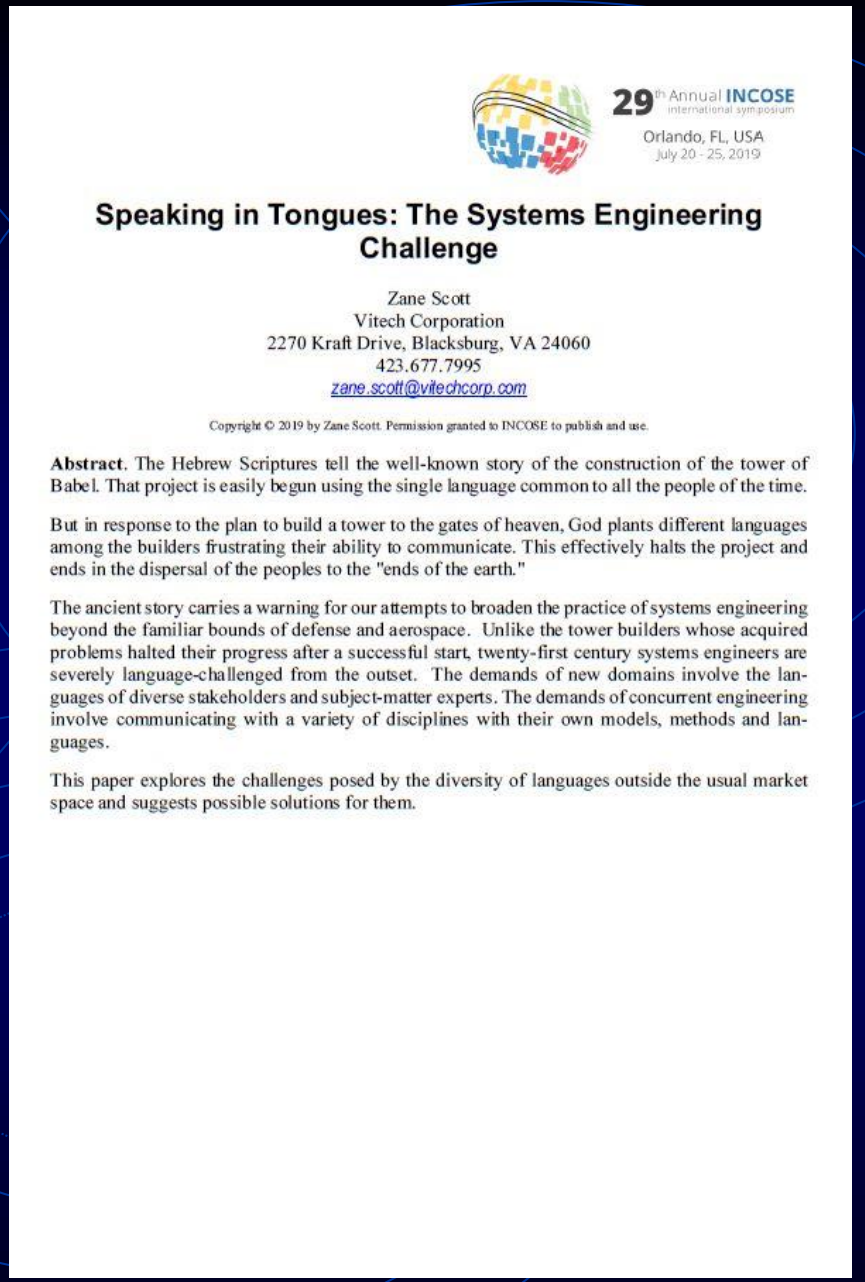
System Complexity Tier	*Characterized by*
Simple	Solution does not required an engineered system
Complicated	Assembly of static parts
Complex	Interactions of dynamic operations
Complex Adaptive	Application of Artificial Intelligence determining system responses
WICKED Systems	Not all the inputs are documented or well-described

- The potentially infinite diversity of complex system examples precludes a 'one-size-fits-all' mentality when it comes to responsible and responsive Systems Engineering approaches to working with complexity.
- Much has been written on the nature of complexity in engineered systems though there is little consensus on what precisely generates complexity let alone what to do about it - and that can be seen as the general nature of it.

SE Knowledge of Cross Discipline Languages and SE Learning across another Discipline's Methods is crucial to future solutions

- Embraces 3 of the 6 INCOSE 2025 tenets

1. Expanding the APPLICATION of systems engineering across industry domains.
2. Embracing and learning from the diversity of systems engineering APPROACHES.
3. Applying systems engineering to help shape policy related to Social And Natural Systems. (INCOSE 2014)



29th Annual INCOSE international symposium
Orlando, FL, USA
July 20 - 25, 2019

Speaking in Tongues: The Systems Engineering Challenge

Zane Scott
Vitech Corporation
2270 Kraft Drive, Blacksburg, VA 24060
423.677.7995
zane.scott@vitechcorp.com

Abstract. The Hebrew Scriptures tell the well-known story of the construction of the tower of Babel. That project is easily begun using the single language common to all the people of the time.

But in response to the plan to build a tower to the gates of heaven, God plants different languages among the builders frustrating their ability to communicate. This effectively halts the project and ends in the dispersal of the peoples to the "ends of the earth."

The ancient story carries a warning for our attempts to broaden the practice of systems engineering beyond the familiar bounds of defense and aerospace. Unlike the tower builders whose acquired problems halted their progress after a successful start, twenty-first century systems engineers are severely language-challenged from the outset. The demands of new domains involve the languages of diverse stakeholders and subject-matter experts. The demands of concurrent engineering involve communicating with a variety of disciplines with their own models, methods and languages.

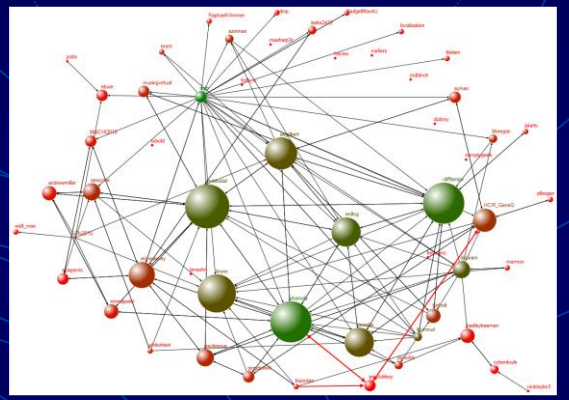
This paper explores the challenges posed by the diversity of languages outside the usual market space and suggests possible solutions for them.

Addressing the 5th Generation Challenge

SE Vision 2025

New Techniques for Engineering a System of Systems

- The Internet of Things extends the SoS challenge beyond interconnected computers and users, to include increasingly interconnected systems and devices that monitor and control everything from household appliances to automobiles.
- A diverse set of stakeholders will increasingly demand SoS to provide information and services, leveraging value from the pieces.
- Techniques for analyzing interactions among independent systems and **understanding emergent behaviors** in SoS must mature.
- **New measures** will be developed **to characterize the SoS**.
- SoSE will **employ new continuous verification methods** as changes occur without central control.
- **Design of experiments** is one such methodology for optimizing a verification program with many parameters and uncertainty.
- **Requirements management will evolve** to address even more diverse stakeholders, in the face of uncertain organizational authority.
- **Methods for making evolutionary interoperability** agreements among SoS constituents will become more robust.



Collaborative Engineering

SE Vision 2025

- In 2025 and beyond, systems engineering will be a key integrator role for collaborative enterprise engineering ***that span regions, cultures, organizations, disciplines, and life cycle phases.***
- This will result ***in multi-disciplinary engineering workflows*** and data being integrated to support agile program planning, execution, and monitoring.
- The collaboration will extend across the supply chain so that customers, primes, subcontractors, and suppliers are integrated throughout all phases of development
- ***Automated workflow, data integration, and networked communications are critical*** to agile program execution, such as when implementing a change process.

2017 IEEE Conference on Standards for Communications and Networking (CSCN)

5G Security: Analysis of Threats and Solutions

Ijaz Ahmad*, Tanesh Kumar†, Madhusanka Liyanage‡, Jude Okwuibe§, Mika Ylianttila¶, Andrei Gurtov‖
*†‡§¶Centre for Wireless Communications, University of Oulu, Finland
‖ Department of Computer and Information Science, Linköping University, SE-581 83 Linköping, Sweden
Email: {*Ijaz.Ahmad,†Tanesh.Kumar‡Madhusanka.Liyanage§Jude.Okwuibe ¶Mika.Ylianttila}@oulu.fi
‖gurtov@acm.org

***Abstract*—5G will provide broadband access everywhere, entertain higher user mobility, and enable connectivity of massive number of devices (e.g. Internet of Things (IoT)) in an ultra-reliable and affordable way. The main technological enablers such as cloud computing, Software Defined Networking (SDN) and Network Function Virtualization (NFV) are maturing towards their use in 5G. However, there are pressing security challenges in these technologies besides the growing concerns for user privacy. In this paper, we provide an overview of the security challenges in these technologies and the issues of privacy in 5G. Furthermore, we present security solutions to these challenges and future directions for secure 5G systems.**

***Index Terms*—Security; 5G Security; SDN; NFV; Cloud; Privacy; Communication Channels**

I. Introduction

The vision of 5G wireless networks lies in providing very high data rates and higher coverage through dense base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency [1]. To provide the necess
service de
be require
operators t
owning the
clouds usi
distinct sy
vices can t
and availal
Operationa
Softwari
bility and
vices. Soft
function s
data forwa
through ab
manageme
ization (NI
functions i
eliminates
SDN and
work elast
break the t
thus are o
with these
and user p

Wireless communication systems have been prone to security vulnerabilities from the very inception. In the first generation (1G) wireless networks, mobile phones and wireless channels were targeted for illegal cloning and masquerading. In the second generation (2G) of wireless networks, message spamming became common not only for pervasive attacks but injecting false information or broadcasting unwanted marketing information. In the third generation (3G) wireless networks, IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains. With the increased necessity of IP based communication, the fourth Generation (4G) mobile networks enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. This development led to more complicated and dynamic threat landscape. With the advent of the fifth generation (5G) wireless networks, the security threat vectors will be bigger than even before with greater concern for privacy.

Therefore, it is crucial to highlight the security challenges

Table II
SECURITY TECHNOLOGIES AND SOLUTIONS

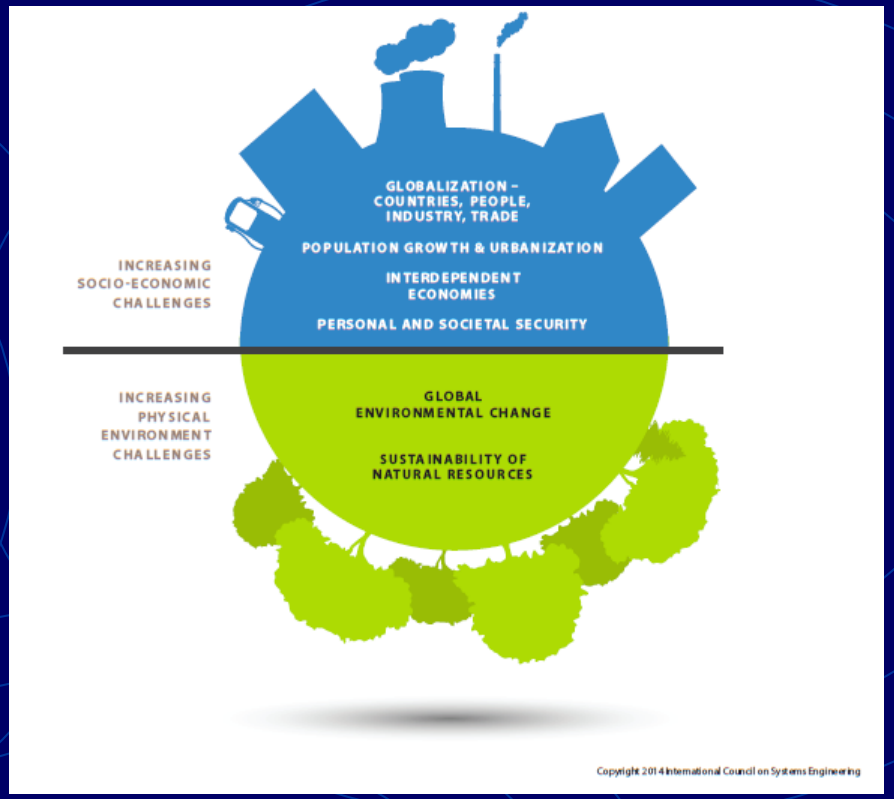
Security Technology	Primary Focus	Target Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS, DDoS detection [34], [35]	Security of centralized control points	✓	✓			
Configuration verification [36], [37]	Flow rules verification in SDN switches	✓				
Access control [38], [39] [40]	Control access to SDN and core network elements	✓	✓		✓	
Traffic isolation [41]	Ensures isolation for VNFs and virtual slices		✓			
Link security [42], [24], [43]	Provide security to control channels	✓		✓		
Identity verification [44], [45], [46]	User identity verification for roaming and clouds services					✓
Identity security [47], [48]	Ensure identity security of users					✓
Location security [26], [27]	Ensure security of user location					✓
IMSI security [49]	Secure the subscriber identity through encryption					✓
Mobile terminal security [7]	Anti-maleware technologies to secure mobile terminals					✓
Integrity verification [50]	Security of data and storage systems in clouds				✓	
HX-DoS metigation [9]	Security for cloud web services				✓	
Service access Control [51]	Service-based access control security for clouds				✓	

978-1

Important 2017 IEEE Paper from Universities in Finland & Sweden proposes potential solutions for 5G Security Threats

https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions

Addressing the Infrastructure Challenge



SE Vision 2025 identifies infrastructure and interdependence of technology-global trends as key drivers of future systems

Global trends include changes to both socio-economic conditions and changes in our physical environment. These global changes impose new demands on the types of systems that are needed, yet are often impacted by the very technology and system developments meant to satisfy the human needs.

For example, increased population growth and urbanization impose new challenges on transportation, health, and other modern infrastructures, while at the same time, systems solutions and technology itself can adversely impact air and water quality

The global community is calling for more attention to how systems can positively contribute to our social condition and natural environment to help advance our quality of life.

Leadership & Planning

ASCE's Grand Challenge

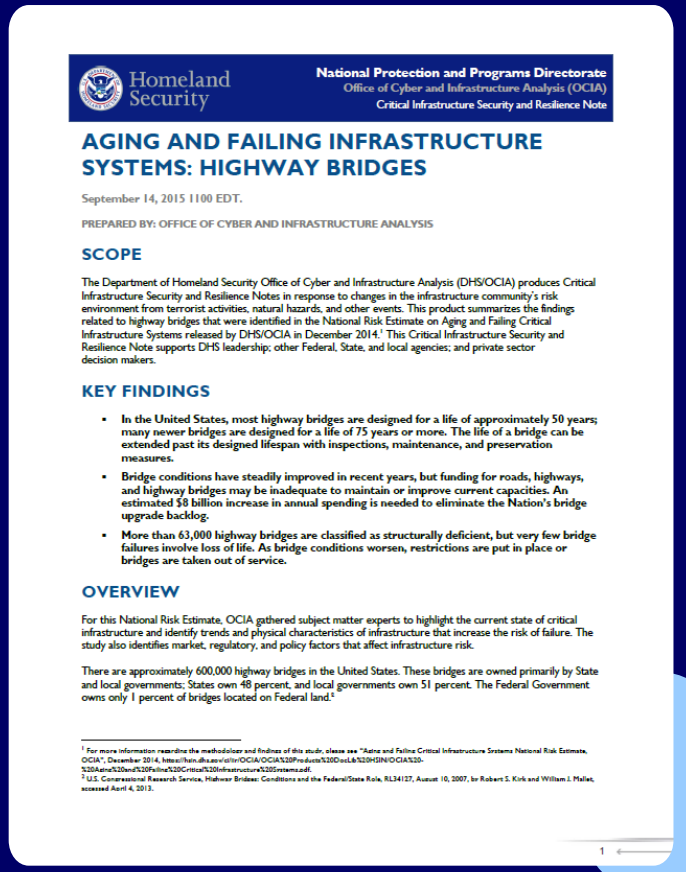
- ***Smart investment will only be possible with leadership, planning, and a clear vision for our nation's infrastructure.*** Leaders from all levels of government, business, labor, and ***nonprofit organizations*** must come together to ensure all investments are spent wisely, prioritizing projects with critical benefits to the economy, public safety, and quality of life.
- **To do so, we must:**

1. Require all projects greater than $5 million that receive federal funding use life cycle cost analysis and develop a plan for funding the project, including its maintenance and operation, until the end of its service life.
2. Create incentives for state and local governments and the private sector to invest in maintenance, and to improve the efficiency and performance of existing infrastructure.
3. ***Develop tools*** to ensure that projects most in need of investment and maintenance are prioritized.
4. ***Streamline the project permitting process*** across infrastructure sectors, with safeguards to protect the natural environment, to provide greater clarity to regulatory requirements, bring priority projects to reality more quickly, and secure cost savings.
5. ***Identify a pipeline of infrastructure projects attractive to private sector investment*** and public-private partnership.
6. ASCE recognizes civil engineers' unique leadership role in addressing our infrastructure challenges. ASCE issued its "Grand Challenge," a call to action for the entire civil engineering profession to increase the value and capacity of infrastructure and increase and optimize infrastructure investments.
7. Central to the Grand Challenge is a commitment to rethinking what's possible through life cycle cost assessments, innovation, performance-based standards, and enhanced resiliency, with ***the goal of reducing the life cycle cost of infrastructure by 50 percent by 2025.***

https://www.infrastructurereportcard.org/solutions/leadership-planning/

CISA Established November 16, 2018

- Cybersecurity and Infrastructure Security Agency
- Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society.
- On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).



Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

AGING AND FAILING INFRASTRUCTURE SYSTEMS: HIGHWAY BRIDGES

September 14, 2015 1100 EDT.

PREPARED BY: OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

SCOPE

The Department of Homeland Security Office of Cyber and Infrastructure Analysis (DHS/OCIA) produces Critical Infrastructure Security and Resilience Notes in response to changes in the infrastructure community's risk environment from terrorist activities, natural hazards, and other events. This product summarizes the findings related to highway bridges that were identified in the National Risk Estimate on Aging and Failing Critical Infrastructure Systems released by DHS/OCIA in December 2014.[1] This Critical Infrastructure Security and Resilience Note supports DHS leadership; other Federal, State, and local agencies; and private sector decision makers.

KEY FINDINGS

- In the United States, most highway bridges are designed for a life of approximately 50 years; many newer bridges are designed for a life of 75 years or more. The life of a bridge can be extended past its designed lifespan with inspections, maintenance, and preservation measures.
- Bridge conditions have steadily improved in recent years, but funding for roads, highways, and highway bridges may be inadequate to maintain or improve current capacities. An estimated $8 billion increase in annual spending is needed to eliminate the Nation's bridge upgrade backlog.
- More than 63,000 highway bridges are classified as structurally deficient, but very few bridge failures involve loss of life. As bridge conditions worsen, restrictions are put in place or bridges are taken out of service.

OVERVIEW

For this National Risk Estimate, OCIA gathered subject matter experts to highlight the current state of critical infrastructure and identify trends and physical characteristics of infrastructure that increase the risk of failure. The study also identifies market, regulatory, and policy factors that affect infrastructure risk.

There are approximately 600,000 highway bridges in the United States. These bridges are owned primarily by State and local governments; States own 48 percent, and local governments own 51 percent. The Federal Government owns only 1 percent of bridges located on Federal land.[2]

[1] For more information regarding the methodology and findings of this study, please see "Aging and Failing Critical Infrastructure Systems National Risk Estimate, OCIA", December 2014, https://hsin.dhs.gov/ci/sites/OCIA/OCIA%20Products%20Docs/L&%20HSIN/OCIA%20-%20Aging%20and%20Failing%20Critical%20Infrastructure%20Systems.pdf.

[2] U.S. Congressional Research Service, Highway Bridges: Conditions and the Federal/State Role, RL34127, August 10, 2007, by Robert S. Kirk and William J. Mallett, accessed April 4, 2015.

1

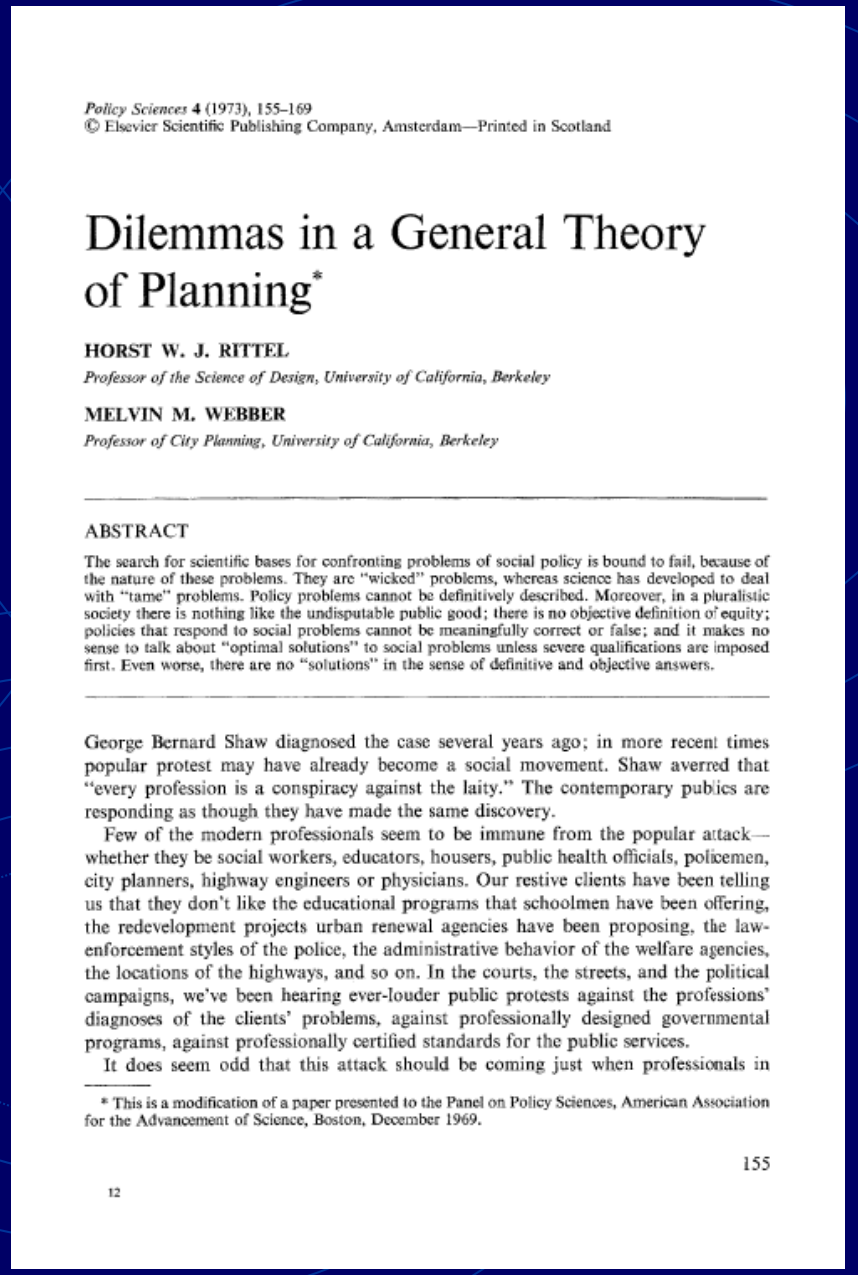
https://publicintelligence.net/dhs-collapsing-bridges/

Wicked Problems

- Definition:

"one of the most intractable problems is that of defining problems (of knowing what distinguishes an observed condition from a desired condition) and of locating problems (finding where in the complex causal networks the trouble really lies)"

- **Planning Problems are Wicked Problems**



Policy Sciences 4 (1973), 155–169

Dilemmas in a General Theory of Planning*

HORST W. J. RITTEL
Professor of the Science of Design, University of California, Berkeley

MELVIN M. WEBBER
Professor of City Planning, University of California, Berkeley

ABSTRACT

The search for scientific bases for confronting problems of social policy is bound to fail, because of the nature of these problems. They are "wicked" problems, whereas science has developed to deal with "tame" problems. Policy problems cannot be definitively described. Moreover, in a pluralistic society there is nothing like the undisputable public good; there is no objective definition of equity; policies that respond to social problems cannot be meaningfully correct or false; and it makes no sense to talk about "optimal solutions" to social problems unless severe qualifications are imposed first. Even worse, there are no "solutions" in the sense of definitive and objective answers.

George Bernard Shaw diagnosed the case several years ago; in more recent times popular protest may have already become a social movement. Shaw averred that "every profession is a conspiracy against the laity." The contemporary publics are responding as though they have made the same discovery.

Few of the modern professionals seem to be immune from the popular attack—whether they be social workers, educators, housers, public health officials, policemen, city planners, highway engineers or physicians. Our restive clients have been telling us that they don't like the educational programs that schoolmen have been offering, the redevelopment projects urban renewal agencies have been proposing, the law-enforcement styles of the police, the administrative behavior of the welfare agencies, the locations of the highways, and so on. In the courts, the streets, and the political campaigns, we've been hearing ever-louder public protests against the professions' diagnoses of the clients' problems, against professionally designed governmental programs, against professionally certified standards for the public services.

It does seem odd that this attack should be coming just when professionals in

* This is a modification of a paper presented to the Panel on Policy Sciences, American Association for the Advancement of Science, Boston, December 1969.

155

12

http://urbanpolicy.net/wp-content/uploads/2012/11/Rittel+Webber_1973_PolicySciences4-2.pdf

'Wicked' Problems have characteristics very different from complex problems

1. There is no definitive formulation of a *wicked problem*
2. *Wicked problems* have no stopping rule
3. Solutions to *wicked problems* are not true-or-false, but good-or-bad
4. There is no immediate and no ultimate test of a solution to a *wicked problem*
5. Every solution to a *wicked problem* is a "one-shot operation"; because there is no opportunity to learn by trial-and-error, every attempt counts significantly
6. *Wicked problems* do not have an enumerable (or an exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan
7. Every *wicked problem* is essentially unique
8. Every *wicked problem* can be a symptom of another problem.
9. The existence of a discrepancy representing a *wicked problem* can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution
10. Because of the *social consequences*, the planner has no margin for being wrong unlike the situation when a scientist makes a scientific hypothesis.

http://urbanpolicy.net/wp-content/uploads/2012/11/Rittel+Webber_1973_PolicySciences4-2.pdf

Dealing in earnest with a ‘Wicked’ Problem

- The “Science Of Muddling Through”—- not an elegant sounding engineering method, but it’s scientific, adaptive, legitimate and just may be our best option
- The paper identifies the best way to address Wicked Problems—- dive into the middle, work locally, solve what you can, keep working to the edges..... this is a radical shift in systems engineering
- Some solutions were out there in other disciplines and only need to be revisited
- The Science of Muddling Through is an elixir for some wicked problems.

The Science of “Muddling Through”

By CHARLES E. LINDBLOM

Associate Professor of Economics
Yale University

➤ Short courses, books, and articles exhort administrators to make decisions more methodically, but there has been little analysis of the decision-making process now used by public administrators. The usual process is investigated here—and generally defended against proposals for more "scientific" methods.

Decisions of individual administrators, of course, must be integrated with decisions of others to form the mosaic of public policy. This integration of individual decisions has become the major concern of organization theory, and the way individuals make decisions necessarily affects the way those decisions are best meshed with others'. In addition, decision-making method relates to allocation of decision-making responsibility—who should make what decision.

More "scientific" decision-making also is discussed in this issue: "Tools for Decision-Making in Resources Planning."

SUPPOSE an administrator is given responsibility for formulating policy with respect to inflation. He might start by trying to list all related values in order of importance, e.g., full employment, reasonable business profit, protection of small savings, prevention of a stock market crash. Then all possible policy outcomes could be rated as more or less efficient in attaining a maximum of these values. This would of course require a prodigious inquiry into values held by members of society and an equally prodigious set of calculations on how much of each value is equal to how much of each other value. He could then proceed to outline all possible policy alternatives. In a third step, he would undertake systematic comparison of his multitude of alternatives to determine which attains the greatest amount of values.

In comparing policies, he would take advantage of any theory available that generalized about classes of policies. In considering inflation, for example, he would compare all policies in the light of the theory of prices. Since no alternatives are beyond his investigation, he would consider strict central control and the abolition of all prices and markets on the one hand and elimination of all public controls with reliance completely on the free market on the other, both in the light of whatever theoretical generalizations he could find on such hypothetical economies.

Finally, he would try to make the choice that would in fact maximize his values.

An alternative line of attack would be to set as his principal objective, either explicitly or without conscious thought, the relatively simple goal of keeping prices level. This objective might be compromised or complicated by only a few other goals, such as full employment. He would in fact disregard most other social values as beyond his present interest, and he would for the moment not even attempt to rank the few values that he regarded as immediately relevant. Were he pressed, he would quickly admit that he was ignoring many related values and many possible important consequences of his policies.

As a second step, he would outline those relatively few policy alternatives that occurred to him. He would then compare them. In comparing his limited number of alternatives, most of them familiar from past controversies, he would not ordinarily find a body of theory precise enough to carry him through a comparison of their respective consequences. Instead he would rely heavily on the record of past experience with small policy steps to predict the consequences of similar steps extended into the future.

Moreover, he would find that the policy alternatives combined objectives or values in different ways. For example, one policy might offer price level stability at the cost of some

SE Thought Provokers

- Does the INCOSE Boundary Definition of a System need to be amended?
- Does recognition of underlying order in apparently random, chaotic activities allow the possibility of limited prediction and/or control?
- Do we have a chance of designing and building an effective Control System for a Superintelligence?
- Will the ubiquity of 5th Generation comms from all kinds of devices and systems overwhelm our ability to effectively respond to anything within a digital world blanketed by unceasing queries, requests, and communications?
- WHO really thinks it is their job to solve the Aging Infrastructure problem?

Conclusions

Artificial Intelligence

- AI has the real potential to result in a National crisis.
- SE Vision 2025 only generally addresses AI, but smart people are out there working it.
- Members' papers on new adaptive methods are specific and focused about the engineering way ahead.
- AI is still a specialized discipline that more Systems Engineers need to be knowledgeable or expert about.
- INCOSE should be addressing the future AI training needs for all SEs.

5th Generation Communications Ubiquity

- INCOSE is addressing this threat through its focus on Cyber Security, Virtual Engineering, and SoS.
- INCOSE should be addressing the future 5G training needs for all SEs

Aging Infrastructure

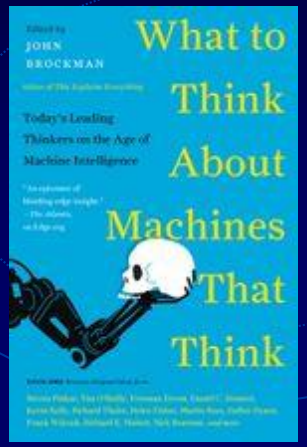
- This problem haunts us all because of funding and needed government leadership. Could INCOSE be better engaged?
- Aging Infrastructure, Porous 5G networks, and AI will interact with crisis results.

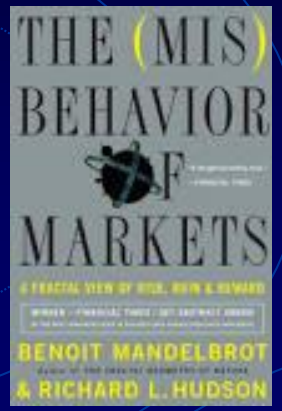
Takeaways

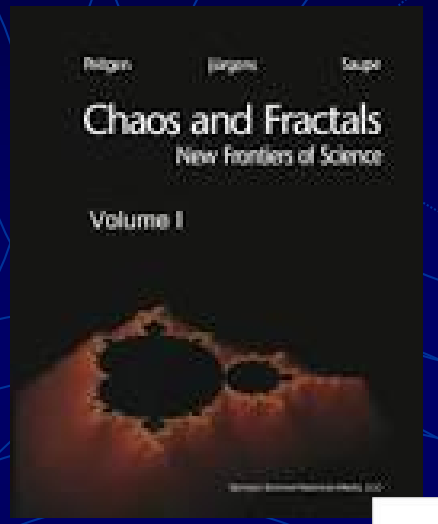
- Not all engineering problems will be linear, self-contained, or well-bounded. i.e. we are solidly in the era of the non-linear, unbounded engineering problem and it is challenging our ability to solve problems using older methods.
- Current Adaptive, Model-Based SE is the correct approach for addressing complexity, and delivering quality, SE solutions.
- SEs will always need to learn new methods and keep learning new methods to tackle today's problems.

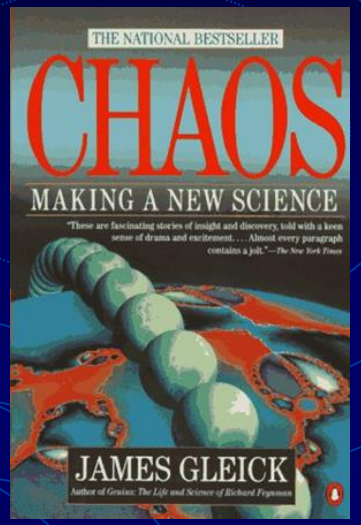
Books

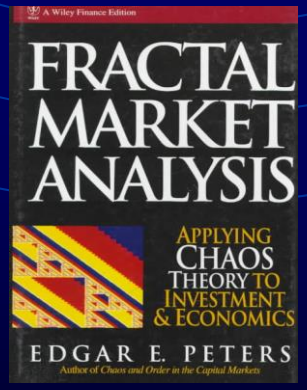
These books are cited throughout the presentation

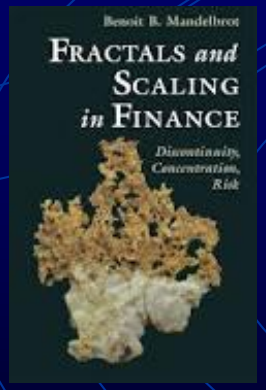


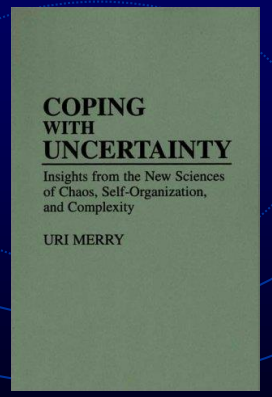


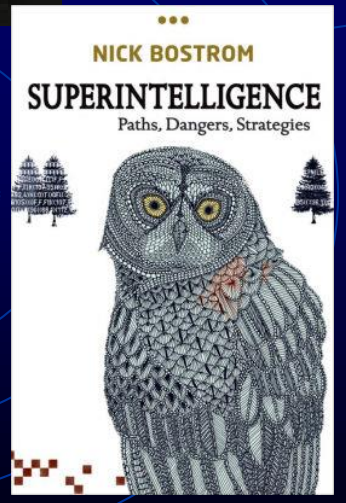












Notes, Books and References

- Lindblom, The Science of "Muddling" Through, 1959
- http://urban.hunter.cuny.edu/~schram/lindblom1959.pdf
- Wikipedia and Intellipedia are cited throughout the presentation
- Any uncited images are coordinated through Google's Image Search and have either Public Domain or Fair Use usage rights associated with the image.

- https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions
- https://www.cns.nyu.edu/~david/handouts/linear-systems/linear-systems.html
- https://www.digitaltrends.com/features/top-10-bad-tech-predictions/
- http://urbanpolicy.net/wp-content/uploads/2012/11/Rittel+Webber_1973_PolicySciences4-2.pdf
- https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/Grades-Chart.png
- https://www.infrastructurereportcard.org/solutions/leadership-planning/

Papers

These papers are cited throughout the presentation

- Ahmad, Ijaz & Kumar, Tanesh & Liyanage, Madhusanka & Okwuibe, Jude & Ylianttila, Mika & Gurtov, Andrei. (2017). 5G Security: Analysis of Threats and Solutions. 10.1109/CSCN.2017.8088621.

- https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/

https://www.howtogeek.com/423720/how-worried-should-you-be-about-the-health-risks-of-5g/