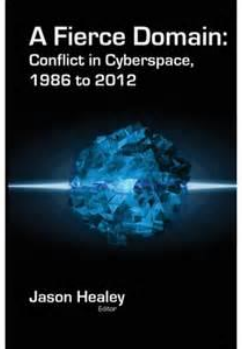


Cyber Resilience of Mobile Systems in an Age of Accelerating Change

Linton Wells II

Avascent Senior Advisor

November 16, 2018

linwells@gmail.com, +1.202.436.6354

Outline

- Presentation is divided into 4 parts
  - What is resilience and how do you build it?
  - The “Age of Accelerations”
  - Planning and engineering for resilience
  - Cyber resilience of mobile systems

linwells@gmail.com, +1.202.436.6354

Definition of Resilience

- Not just bouncing back to status quo *ante*

- Judith Rodin—former head, Rockefeller Foundation:
  - The capacity of any entity –
    - an individual, a community, an organization, or a natural system
  - to prepare for disruptions, to recover from shocks and stresses,
  - and then to adapt and grow from a disruptive experience

- Two critical concepts—must be built by leadership
  - Organizational capacity
  - Ability to adapt and grow

- "Be prepared to bounce forward better"

linwells@gmail.com, +1.202.436.6354

A Profile of Resilience
(Be Prepared to Bounce Forward Better)

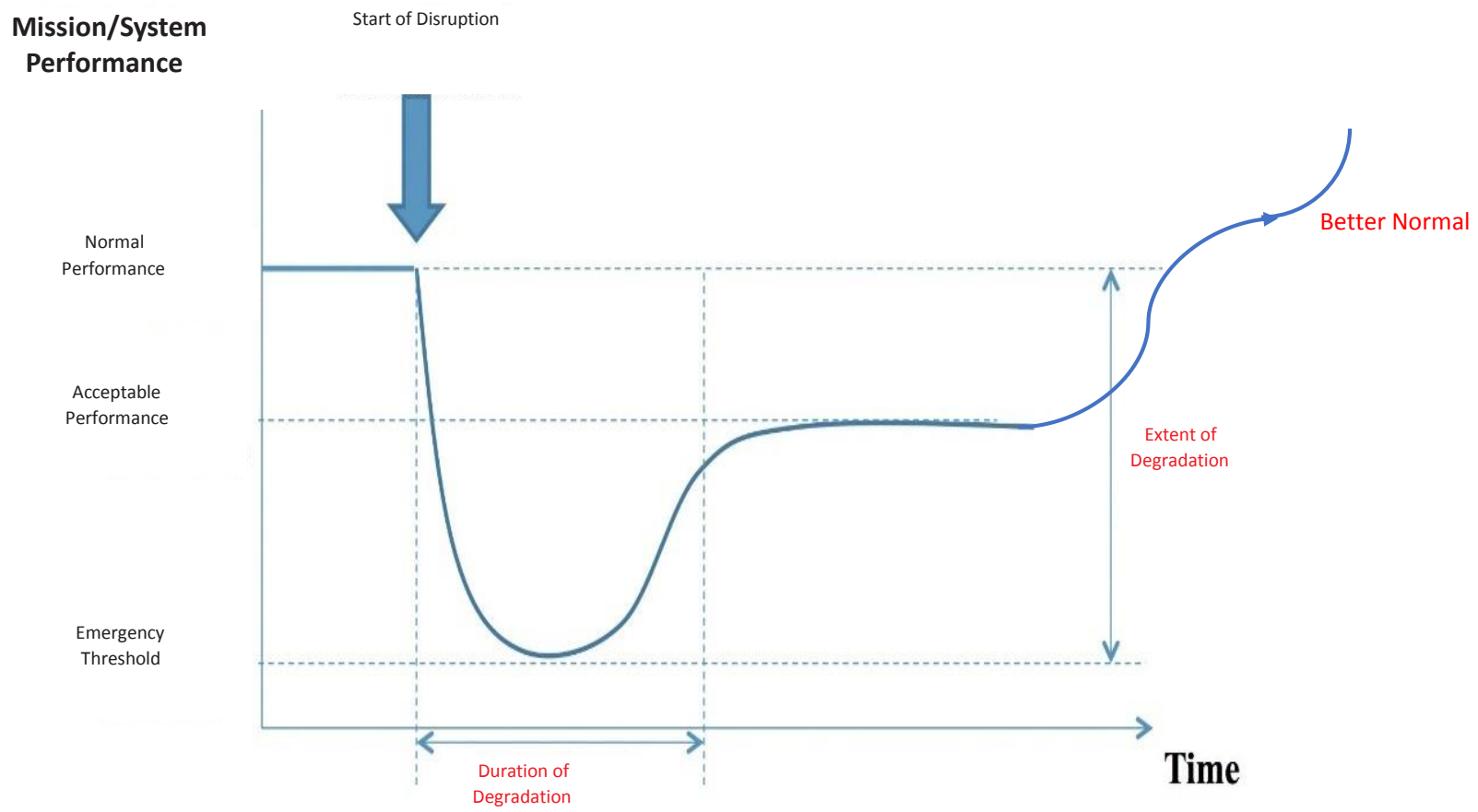


Figure 1. Conceptual diagram for measuring vulnerability and resilience (expanded from KANG Shian Chin, et. al. (2014); based on Richards, Ross, Shah, & Hastings, 2009

Security vs Resilience

- Security is about:
  - "locking up and hunkering down"
- Resilience is about:
  - Achieving organization's goals
  - Under any level of shock or stress
  - Fighting back
  - Emerging stronger

linwells@gmail.com, +1.202.436.6354

Mission Assurance

- DoD Mission Assurance concept is close to resilience
- Protection during
  - Program design
  - Life cycle (supply chain risk management, cyber & physical security, etc.), and
  - Decommissioning
- Goal is to absorb shocks, “fight hurt,” and restore quickly
  - Not just by tactical approaches, but through
    - design
    - configuration control, and
    - rigorous training
    - at all levels

Cultural & Operational Resilience

- Cultural resilience: “maintain composure and keep fighting regardless of situation”
  - Culture must promote resilience--long term perspective
  - Resilient labor force key
- Operational (business) resilience: technology & systems
  - Cybersecurity makes networks & systems more resilient
  - Protect critical infrastructure
  - Use Cross-Functional Teams (CFT) across stovepipes
  - Engage proactively outside—cross-cutting collaboration

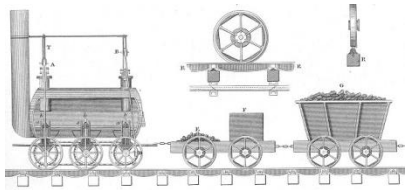
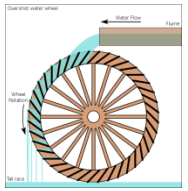
linwells@gmail.com, +1.202.436.6354

Age of Accelerations

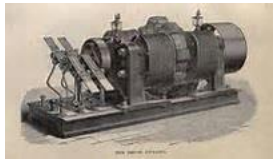
linwells@gmail.com, +1.202.436.6354

Four Industrial Revolutions

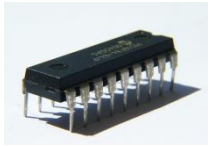
- 1st ~1780s:


- 2nd ~1870:




- 3rd ~1969:



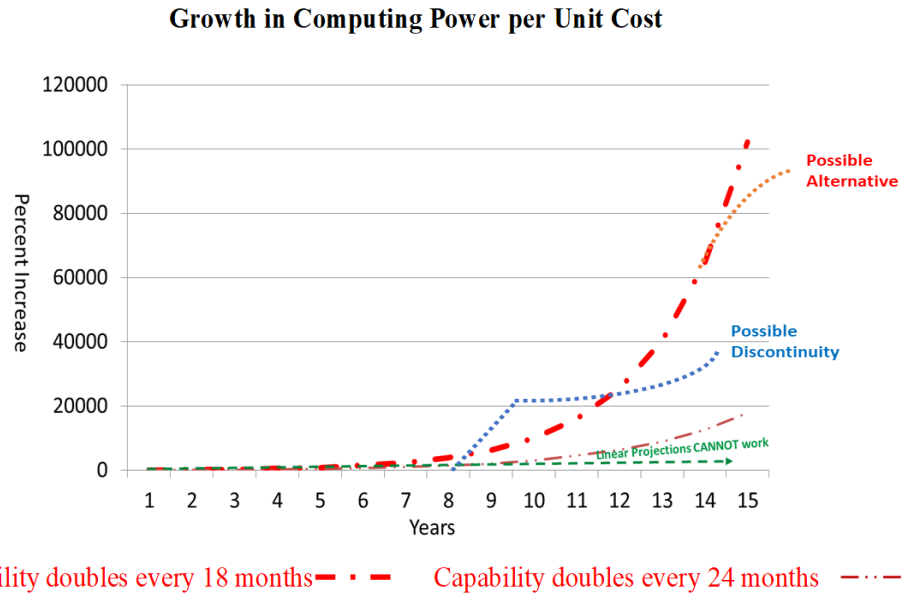
- 4th just beginning: fuse technologies "blur lines between physical, digital and biological spheres"




Source: Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," 14 January 2016 http://www.weforum.org/agenda/2016/01/, accessed February 16, 2016

Velocity of Tech Change

If a factor, e.g. computing power/unit cost, doubles every 18 mo, 5 yr increase is 900%, 10 yr 10,000%, 15 yr ~100,000%



Biotech even faster, robotics ubiquitous, nano poised breakout, energy impacts are global

- Think BRINE (bio-robo-info-nano-energy) + Additive Manufacturing & AI

Interactions complicate things

Linear projections CAN'T work

Cyber Resilience

linwells@gmail.com, +1.202.436.6354

Key Points

- A cyber-resilient organization must be part of an organization that is resilient overall
- Cybersecurity contributes to cyber resilience, but cyber resilience is much broader
- Need to address more than just technical cyber issues—also consider cultural and information components

Cyber Attack Chain

cyberwarzone.com

OODA Loop & Decision Cycles

- "Observe" and "Orient" phases increasingly electromagnetic
- "Decide" and "Act" supported by information processing
- Cyber can dominate OODA loop in all domains
- Tech changes
  - Processing power
  - Machine learning
  - Sensor proliferation
  - Army 2050 battlefield—can you move?
- Speed of decisions
  - "Human-on-the-loop," vice "Human-in-the-loop"

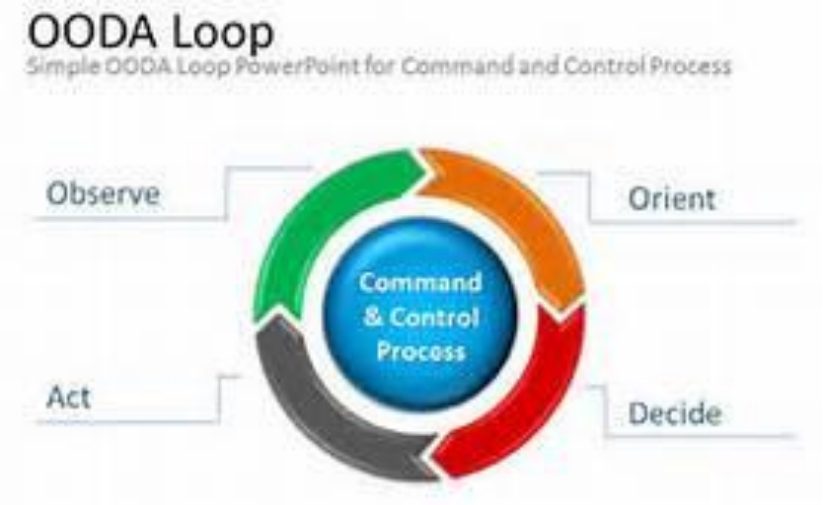


Image courtesy successing.com

linwells@gmail.com, +1.202.436.6354

Cyber Resilience Starting Points

- Malicious cyberspace activities typically include “5Ds:”
  - Deny; Disrupt; Degrade; Destroy; Deceive,
  - Increasingly combining with Information Operations and kinetic actions
- Types of attacks against control systems
  - Attacks on Human Machine Interface (HMI)—200+ vulnerabilities
  - Distributed Denial of Service (DDOS)
    - Moving to Destruction of Service (DeOS)
  - Remote penetration
  - Hardware/firmware modification
  - Supply chain vulnerability
  - Social engineering
  - Cleared insiders
- Must include both Operational Technology (OT) and Information Technology (IT)

linwells@gmail.com, +1.202.436.6354

Analytical Approaches

- System Criticality
  - How critical is a system to overall mission?
  - Consequence-based cybersecurity—don't spend time on inconsequential systems

Know Mission Dependencies to Assure Mission

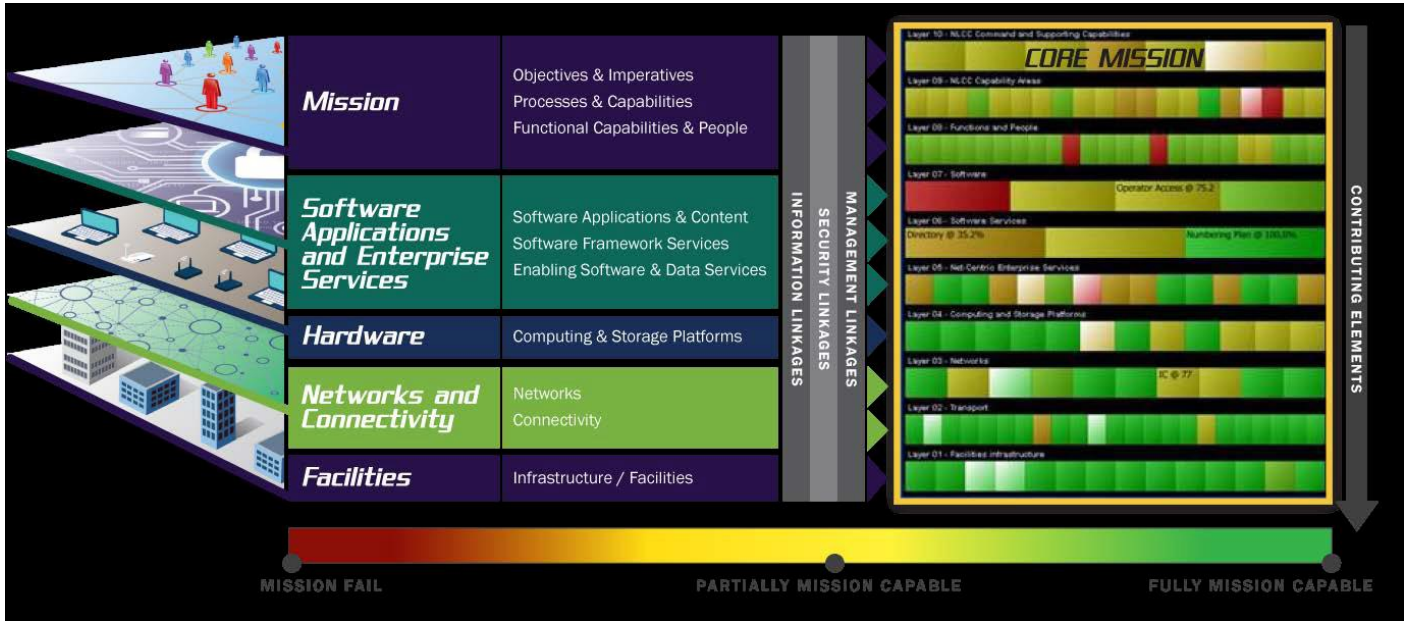


Figure 6: From: Haegley 2018, slide 26

linwells@gmail.com, +1.202.436.6354

Cyber Resilience of Mobile Systems

linwells@gmail.com, +1.202.436.6354

Components of Mobile Systems

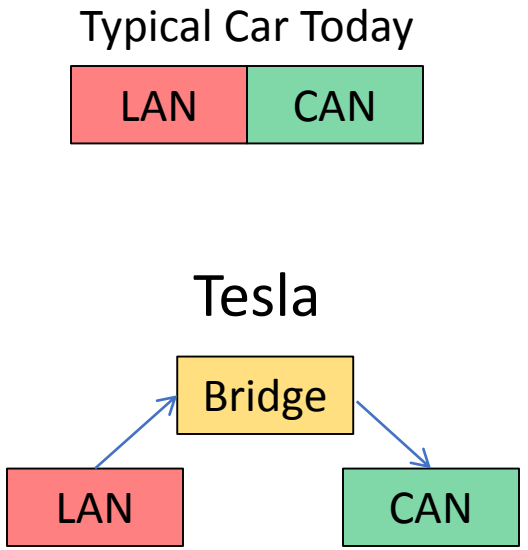
- RF Interfaces
  - Radios, Radars, EW equipment—Cyber-EW convergence
  - Other sensors—tire pressure via Blue Tooth
  - ONSTAR and similar devices
  - Smart vehicle sensors
- Internal Networks
  - Infotainment LAN and CAN in cars
  - IT vs OT (generators, pumps, radars, etc.) in ships
  - 1553 and similar data busses in aircraft
- Control Systems
  - Steering, braking, “smart cruise control,” etc. in cars
  - Navigation, steering and engine controls in ships
  - Command and Control systems
  - Flight controls and avionics
- Actuators
  - Electric, hydraulic, mechanical
- Patching mechanisms

Implementing Cyber Resilience

- Preparations/Mitigation
  - Mission Assurance-like life-cycle approaches
  - Resilient architectures
    - Including spectrum agility and GPS alternatives
  - Trained people—don't forget families
  - Culture of resilience
  - Public-private collaborative mechanisms, and trust, in place
- Near-Real-Time defenses
  - Situational Awareness
  - Decision support and command structure
  - Agile and protected components
  - Supporting C4I
- Post-attack reconstitution
  - "Bounce forward better" to the new environment

Automobile Example

Tesla security architecture shows there IS a secure alternative



Typical car today

- Mixes Infotainment LAN and vehicle control CAN (Controller Area Network)
- Multiple RF paths into LAN
- Hard to patch

Tesla

- Separates LAN & CAN
- Crypto-secure bridge
- Over-the-air fixes

Can Tesla-like “wrapper” be applied to traditional SCADA systems?

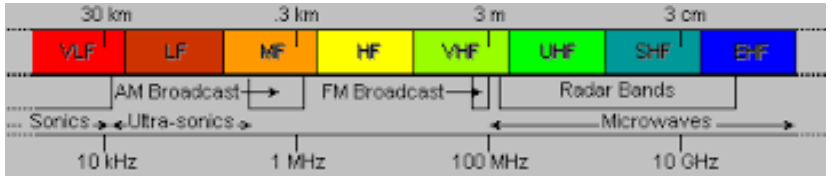
Maritime Example

USN Approach (from TFCA)

- Boundary Control Points and Enclave Segregation
- Cyber Situational Awareness (SA):
- Designing (vice retroactively Patching-in) Resiliency within Systems & Networks:
- Cyber Hygiene: Use of focused Tactics, Techniques & Procedures (TTPs) and workforce training
- Cyber Ready Workforce: Improving manning levels, personnel training and Fleet readiness

Space-Related Considerations

- On-orbit components
  - Proliferating commercial systems add diversity, but likely less secure
  - Can diversify constellation faster
- Transmissions to/from the satellite
  - Don't get fixated on military systems
  - Disruption of GPS will have enormous civilian consequences
  - Spectrum agility

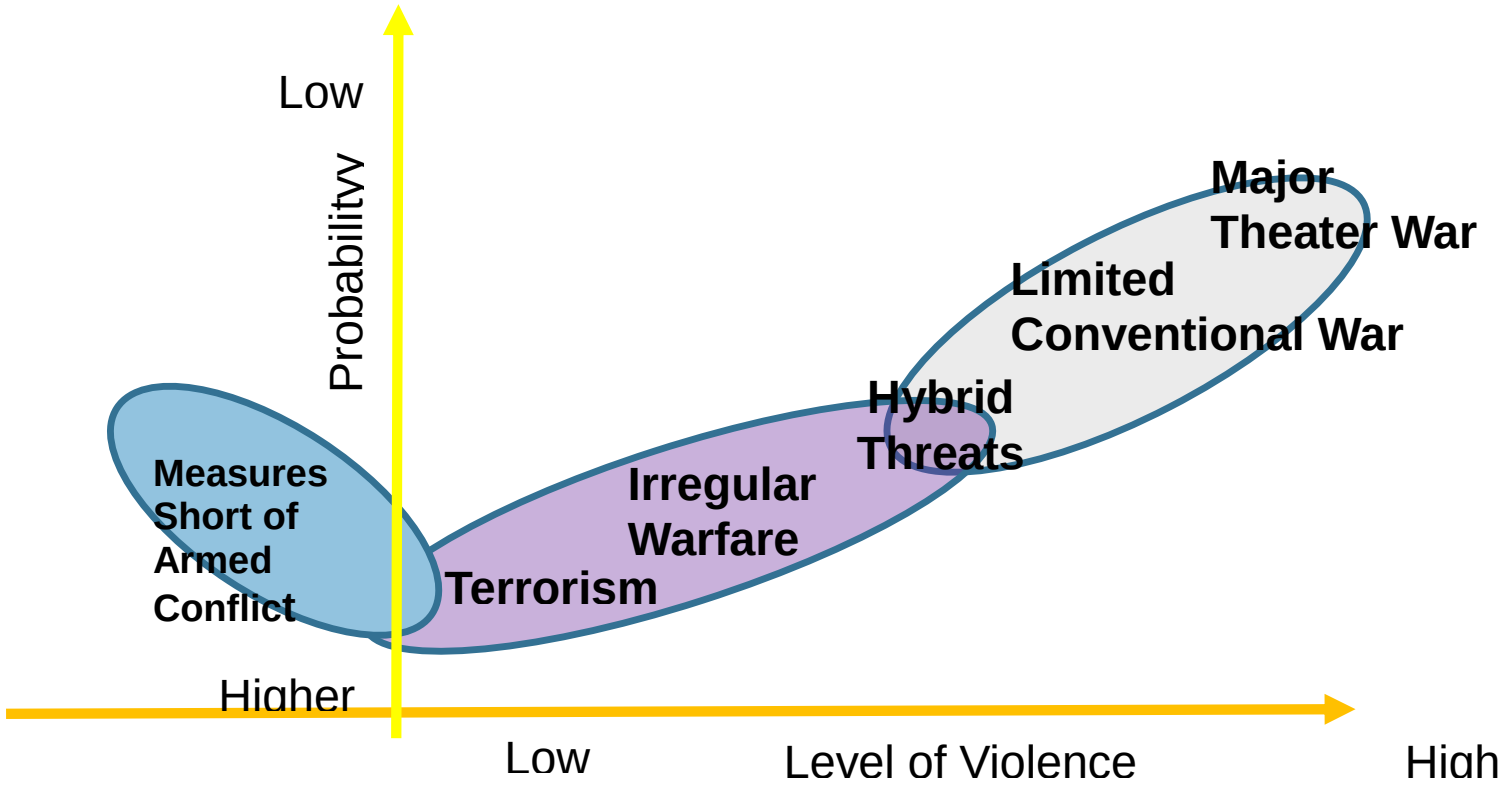


- Ground components (fixed and mobile)
  - Remember supporting components, like commercial power grids
  - Likely to include diverse components

- Cyber attack surface increasing in every area

linwells@gmail.com, +1.202.436.6354

Spectrum of Conflict



From Dr. Frank Hoffman, 2017

Organize, Train, Equip (1)
Prepare for the War, Not Just the Battle

- Non-traditional missions
- Cognitive-Emotional Conflict
- Rapidly changing equipment
- Personnel skills in high demand by private sector
- Need multi-tiered training: leaders, techs, workers
- Difficult policy, ethical, and moral questions
  - Many legal issues—ambiguities in applying Law of Armed Conflict to cyberspace
  - No “rules of the road” for cyberespionage
  - Can only be addressed through bi-lateral and multi-lateral negotiations

Organize, Train, Equip (2)

- Cyber capabilities cut across domains
  - Most techs don't look for cyber causes
  - Operating at policy-technology-sociology interface
- Cyber-EW convergence adds further complexity
  - Doctrinal differences, analog-digital equipment, etc.
- Conflicting exercise objectives
- Iterative approaches
- Cyberspace operations lend themselves to hybrid warfare and measures short of armed conflict
  - Cyber-on-cyber alone is rarely most effective

Opportunities

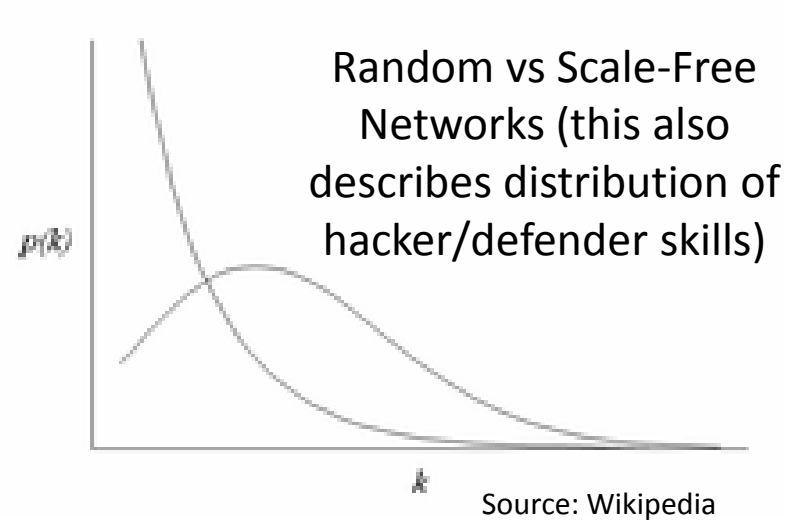
- Implement *Boundary Control Points & Segmented Enclaves*
- Deploy *Cyber Secure Microgrids* for key facilities
- Use *More Secure Codes/Components*, such as formal methods, new approaches to IoT security, and leveraging "cyber risk evaluations"
- Apply *Near-Real Time Anomaly Detection*
- Work toward an *Educated Workforce and Population*
- Incorporate *Artificial Intelligence (AI) & Machine Learning (ML)* effectively – including Explainable AI
- Target resources based on real world threat intelligence

Planning and Engineering for Resilience

- *Multi-Stakeholder* approach:
- Scenarios (set in context) – foresight, vice forecasting
- In analyzing risk—consider:
  - Dependencies, including cross-sector vulnerabilities
  - Cascading casualties; and
  - Overall risk across all dimensions: Physical, Cyber, Human, Temporal
  - Can measure much of this quantitatively
- Examine stakeholder perceptions --adversary's likely to be different than ours
- *Change behaviors through* training, exercises, education and incentives
- ACT EARLY. Designing in is almost always better than adding on afterwards

Next Steps

- True talent is scarce
  - Recognize top group
- AI & Machine Learning
  - Bridge training shortfall
  - Be suspicious of hype
  - Don’t forget cybersecurity of AI & ML algorithm
- Train, train, train—include tough scenarios
- Big data analytics—learn how to use it
- New personnel policies—get access to non-traditional talent
- Include OT-IT intersections



Random vs Scale-Free Networks (this also describes distribution of hacker/defender skills)

Source: Wikipedia

Questions Very Welcome

linwells@gmail.com

Skype: linwells

U.S. cell +1 202.436.6354