Overcoming Markets for Lemons in ICT Products and Services: Metrics, Labelling, and Policy

John C. Mallery (jcma@mit.edu)
WFA Group, LLC

Invited presentation at *the 2021 C3E Conference on Supply Chain Cyber Defense,* October 27-28, 2021.

Version: 10/28/21 4:36 PM

Overview

- *Problem:* Market Failures for Cyber Security and Resilience
- *Solution:* Enable Market Scaling by Monetizing Cyber Security & Resilience
- Multipliers In ICT Production
- Strategy Informed by Work Factor Analysis (WFA)
- Work Factor Engineering (WFE)
- Dimensions of Work Factor Analysis
- Metrics For Cyber Security And Resilience
- 15 Policy Levers for Incentivizing Better Assurance and Resilience
- Policy: Prioritize Efforts to Achieve Work Factor Impact on Adversaries

Problem: Market Failures for Cyber Security and Resilience

Economic Issues

- Risk transfer downstream
  - Customers bear costs but are not able to reengineer flawed architectures
  - Producer business models based on risk transfer
- Market for lemons – buyers will not pay for better security
  - Asymmetric information about information assurance
- Rigid industrial ecosystems with widespread lock-in
  - Outdated architectures
- Difficulties calculating ROI for security and resilience
  - Makes investment decisions difficult

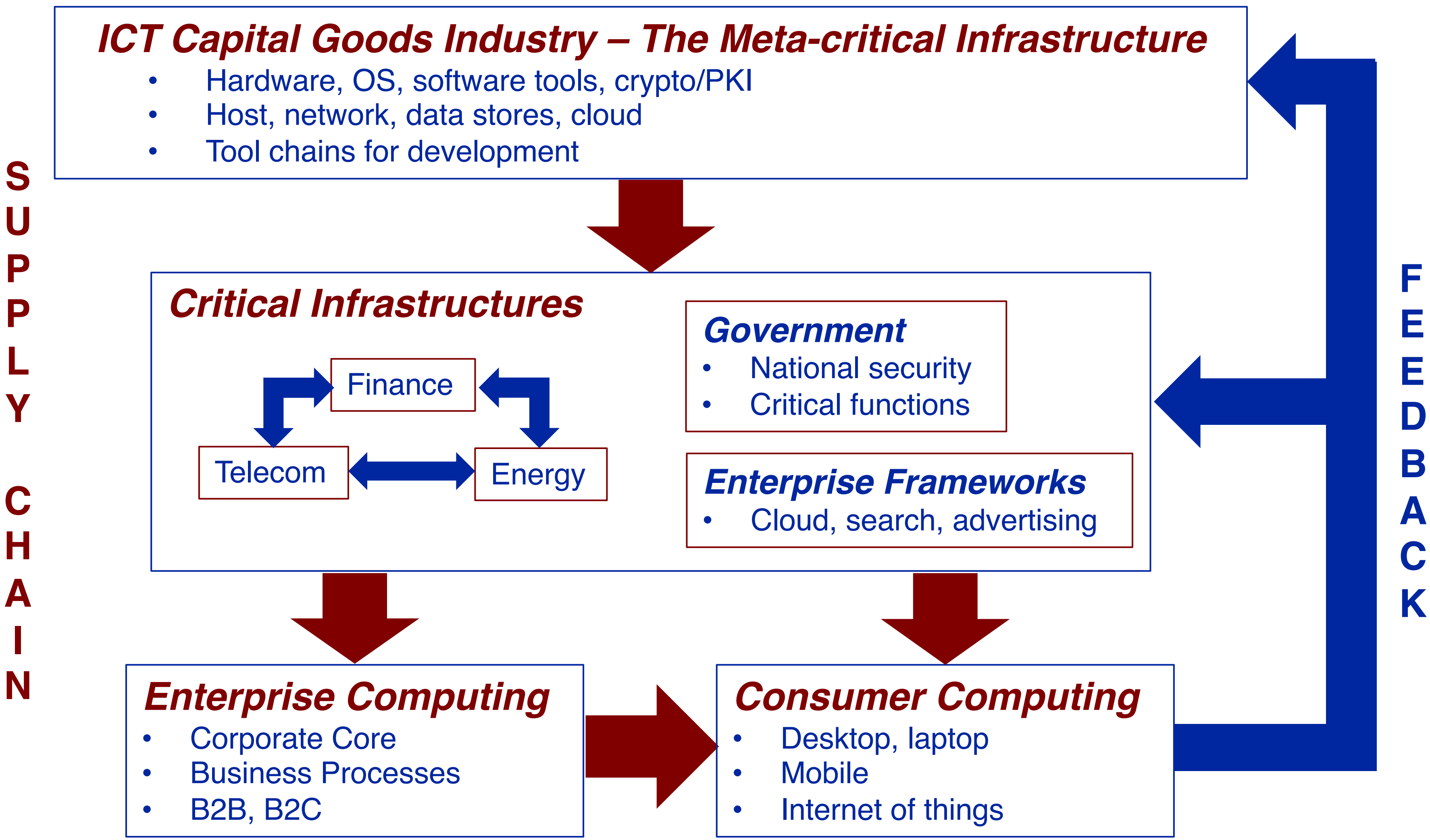
Technical Shortcomings

- Lack of memory safety
  - But, some progress by industry
- Unmanageable complexity
  - Poor architectures fail to optimize locality
- Lack of total system security framework
  - Multi-spectrum attacker
    - Remote access
    - Insiders – witting or unwitting
    - Supply chain
    - Crypto/authorization - subversion of authorization, identity, PKI, side channels, etc.
  - Conservation of threat
  - Enumeration of attack surfaces
- Lack of information flow control enforcement
- Insecure business processes

Solution: Enable Market Scaling by Monetizing Cyber Security & Resilience

- ***Success:***
  - **Market forces spread reasonably high assurance and resilience throughout society and drive continuous innovation (**Precedent: 1990s build out of civilian Internet)
- ***Requirements:***
  - *Metrics:* Ability to accurately measure and compare security and resilience properties
    - Retrodictive metrics
    - **Predictive metrics**
  - *Return on Investment (ROI):* Ability of buyers of IT to reliably understand & measure risk
    - Anticipate, assess, and measure threat levels against the enterprise
    - Estimate losses due to potential cyber attacks
    - **Determine commensurate levels of investment in security & resilience**
  - *Technology Injection:* Transformation of the IT technology plane for security and resilience
    - **Strongly bias work factors in favor of defender against attacker**
    - Dramatically harden systems to prevent intrusions
    - Architect for adaptive resilience and rapid recovery
    - Align security with functionality by making it inherent and largely transparent
    - Radically increase productivity of secure system development, certification, accreditation, and operation
    - Deliver faster development cycles and superior total ownership cost than current generation COTS
  - *Realign Incentives:* Alignment of market incentives for uptake – ultimately next gen COTS
    - **Stratify markets according to assurance needs to provide a learning curve and a path to scale for new transformational technologies**
    - Phased introduction of safety regulations, liability and meaningful cyber insurance as industry is genuinely able to adopt transformational technologies
    - Catalyze ecosystem re-equilibration at higher assurance level
      - Attenuate rigidities in IT capital goods ecosystem that impede technical evolution

Multipliers In ICT Production: From Engines of Vulnerability to Engines of Trust



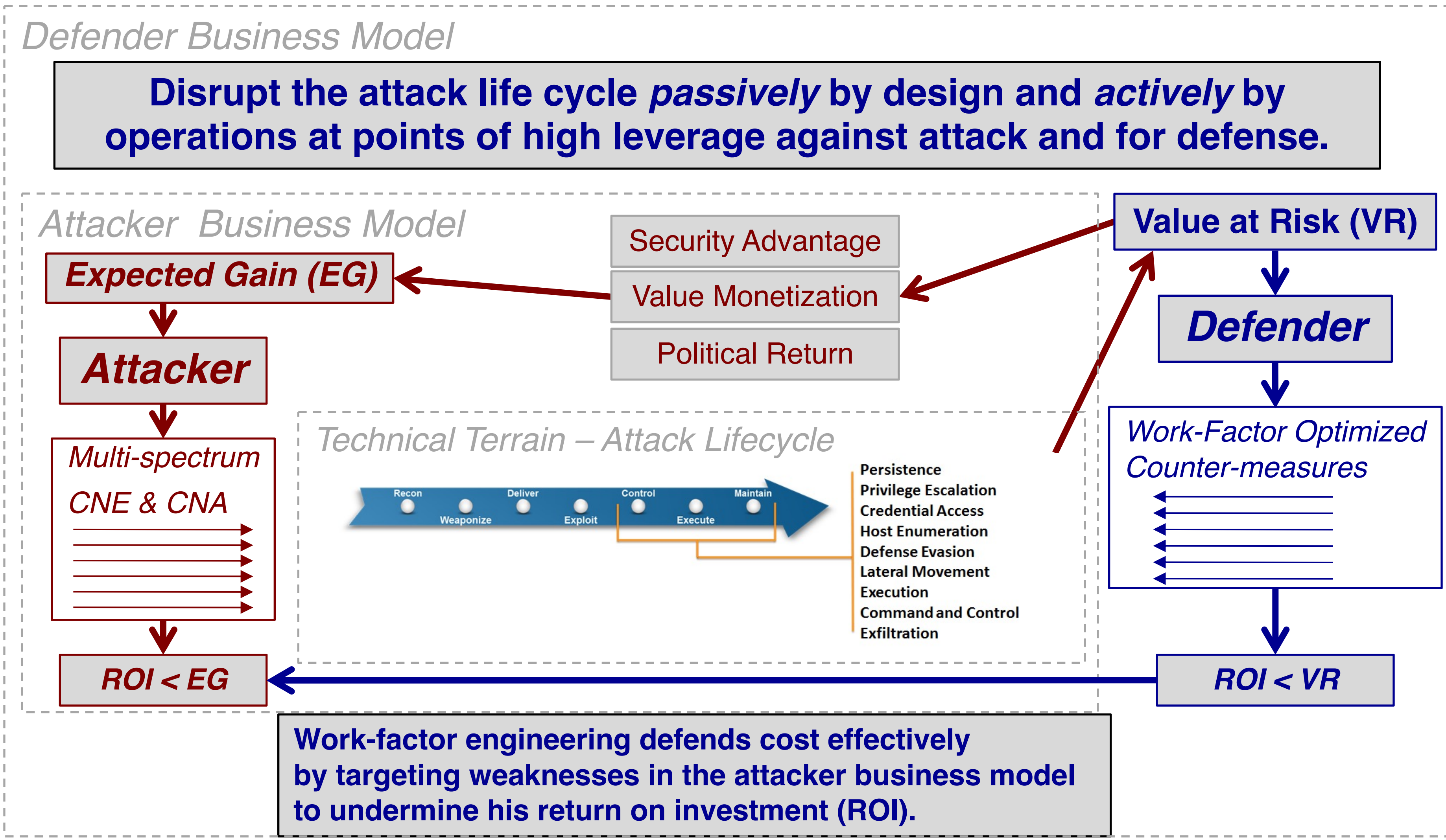
Strategy Informed by Work Factor Analysis (WFA)

- *Goal:* Make technical, operational, or organizational moves that cumulatively:
  - Impose hard problems on attackers (prefer geometric impact)
  - Facilitate coordinated defense (eliminate adverse multipliers)
  - Increase mission risk for attacker
- *Work Factor Analysis (WFA)* characterizes the difficulty of executing tasks
  - Analogous to computational complexity for cryptography
  - Security meta-metric that focuses on difficulty plan elements for attack and defense
  - Extends beyond technical designs to domain embeddings and cyber operations research
  - Relevant for force multiplier estimations
- Distinguish static vs. dynamic defense
  - Security Engineering: System, platform, enterprise
  - Defense in Depth:
    - *Early Warning* – Threat intel; anticipation
    - *Monitoring* – Active checking; detect & track attacker
    - *Intervention* – Correct misconfigurations; Channel & expulse attacker
    - *Learning* – Iterative refinement of system defenses
- *Cyber resilience engineering* requires work factor analysis to compare attack/defense difficulty across modes of recovery, reconstitution
  - Intelligent adversaries move to the weakest attack surface
  - Minimize structure/resource sharing across attacker plans

Work Factor Engineering

Integrates Technical, Organizational, and Economic Perspectives:

The Defender Wins When The Attacker's Expected Gain Is Less Than Attacker's Investment



Dimensions of Work Factor Analysis

- ***Resources***
  - Computational complexity (mathematical leverage)
  - Cost (often related to complexity)
  - Expertise and Knowledge (technical specialties, domain knowledge, human capital)
- ***Planning, Execution, and Information Management***
  - Cognitive difficulty (model as formulation of non-linear plans and counter plans)
  - Learning difficulty (reversing obfuscation, devising new tactics or approaches)
  - Organizational effectiveness/dysfunction (seams, integration, culture, psychology)
- ***Risk***
  - Uncertainty (confidence, incomplete information, bounded rationality)
  - Information differential gain/loss (innovation, leakage by insider, espionage, diffusion)
  - Motivation (cadre, personal or referent group risk)
  - Culture (risk acceptance or aversion)

Metrics For Cyber Security And Resilience

Retrodictive Metrics

- Only recently taken seriously
- Cyber Solarium Commission Recommendation
  - National Cybersecurity Certification and Labeling Authority (Recommendation. 4.1)
    - Product certification and attestation
    - Accredited certifying agents
    - Comparative scoring
- NIST Cybersecurity Labeling Program
  - May 2021 Executive Order 14028 requires consumer labeling for:
    - Internet of Things (IoT) products
    - Secure software development practices
- Retrodiction Paradigm:
  - Identify flaws in technical architectures underlying vulnerabilities in the National Vulnerability Database (NVD)
  - Sequence architectural flaws for correction based on frequency and severity of exploitation
  - Problem: The attacker moves onto new attack surfaces
    - But, likely experiences a higher attack work factor

Predictive Metrics

- Predictive metrics measure a system's ability to resist cyber-attacks, defend against them, or continue to function
  - *Basis:* Formal proofs, computational complexity, statistical likelihoods
- Measurement Tradeoffs:
  - Cost (easy) vs. security (hard)
  - Efficiency (easy) vs. resilience (hard)
- Missing predictive paradigms for:
  - Cyber security
  - Cyber resilience
- Use work factor analysis for cyber security and defense
  - Static resistance
  - Dynamic defense
- Extend work factor analysis for resilience
  - Reconstitution
  - Adaptive range
- Both are infosec grand challenge problems

> *"I cannot scale my investment in security [and resilience] without meaningful predictive metrics." – Dr. Steven King, Associate Director for Information Assurance, Office of the Deputy Under Secretary of Defense for Science & Technology, December 15, 2015.*

15 Policy Levers for Incentivizing Better Assurance and Resilience

National

1. Federal R&D and Procurement
   - Invest in high-leverage security and resilience research and catalyze uptake via procurement
2. Name and Shame
   - Bad publicity around serious cyber breaches
   - Share pressure and CEO firings motivate C-suite responses (e.g., Heartland Payments)
3. Indirect Incentives via Best Practices
   - Industry best practices
   - NIST Cyber Security Framework
   - Certification of conformance to security standards (e.g., Common Criteria, ISO)
4. Insurance Markets
   - Partition market segments based on risk
   - Allocate risk where it can be managed
5. Tax Policy
   - Tax credits for security R&D
   - Tax credits for enterprise defense improvements
   - Accelerated depreciation rates for security modernization
6. Legal Responsibility
   - Criminal actions for egregious negligence
   - Civil actions (Based on phased reduction in liability exemptions)
7. Direct Regulation
   - Telecom, energy, finance, and more

International

8. Trade Incentives - National
   - Block trade in substandard products
   - Penalties for “cyber security pollution”
9. Major Vendor Unilateral Action
   - Intel, Arm, Microsoft, Google, Apple, Cisco
10. Industry Standards for Products and Services
    - TCG Trusted Computing Model (TPM)
11. Voluntary Accords for Sectors
    - Core banks (later Basel Accord?)
    - International Cyber Stability Board?
12. Technology Norms
    - Industry best practices,
    - NIST Cybersecurity Framework
    - NIST Cybersecurity labeling
13. National Regulation based on Standards
    - Nuclear reactor operators, i.e., IAEA
14. Policies of Supranational Entities and Alliances
    - EU, NATO – critical infrastructure
15. World Trade Organization (WTO)
    - Information Technology Agreement
    - Digital Trade Agenda

Policy: Prioritize Efforts to Achieve Work Factor Impact on Adversaries

1. *Cyber Blitz:* Orchestrate strategies that define actual paths to success (Adm. (ret) William O. Studeman)
   - Identify objectives and formulate strategy
   - Socialize the strategy and objectives
   - Organize for success and prioritize effort for impact
   - Gain leverage - use work factor analysis
   - Run fast - realize speed in implementation and exploration of options;
   - Provide effective leadership and governance to drive results across public and private spheres
2. *Research:* Fund Federal R&D programs to develop transformational ICT
   - Work Factor Engineering
     - *Predictive Metrics:* Inform transformational technologies and strategy
     - *Retrodictive Metrics:* Prioritize correction of architectural flaws in deployed systems
     - *Better Information:* Enable market mechanisms to price security & resilience accurately
       - Depends on accurate buyer ROI for security & resilience
   - *Security:* Information Flow Control in the enterprise
     - Ground in Security Tagged Architecture (STA) processors
     - Encapsulate legacy systems and mediate communication on the network and in the host
   - *Resilience:* Self-adaptive computation & networking
3. *Realignment:* Deploy incentives to drive up information assurance & resilience in the current technology plane
   - Prioritize effort based on retrodictive metrics and red teaming
   - Apply Work Factor Engineering across the stack from hardware to business processes
4. *Deployment:* Inject transformational technologies into ICT sectors
   - Examples: Memory safety, zero-trust architectures, and information flow control
   - Drive uptake and scaling of new architectures
     - *Federal Procurement:* $20B in DoD & NSA Cloud contracts to scale STA processor production
     - *Regulation:* Critical infrastructure sectors for energy, telecommunications, finance
     - *Whole-of-Nation:* Private-public partnership
   - Drive down costs through high-productivity secure software engineering
5. *Scale:* Rapidly transition through pilots that can be cloned, tailored, and scaled into other sectors

Appendix

Recommendations

- Launch a **Cyber Blitz**
  - Create *Cyber Strategic Depth* for the nation and strong, resilient, defensible cyber infrastructures for the US military and civilian sectors
  - realize military cyber resilience to dramatically enhance the ability of the US to deter adversaries across all conflict levels and defeat them when necessary.
  - Bring about radical improvements in productivity for software engineering and other ICT design activities will assure US technology leadership

- Technology
  - *Metrics:* Initiate a high-speed research program on work factor analysis and enterprise security engineering
    - Program: Planning for Asymmetric Cyber Advantage (PACA) - 2015
    - Develop multi-spectrum metrics for security and resilience engineering
  - *Systems:* Initiate programs for work-factor informed clean-slate stacks for computing and networking
  - *Handling the Legacy:* Initiate programs to retrofit the legacy with moves that raise adversary work-factor
  - *Uptake Transformational Technologies:* Protect legacy systems via routers, bodyguards, emulators, recompilation, software rewrites

- Industrial Strategy
  - *Start:* Initiate a planning process to move key ICT components, systems, and sectors to higher levels of assurance and resilience
  - *Strategize:* Develop an incentive strategy to catalyze update security and resilience best practices
  - *Modernize:* Deploy transformational technologies in the defense sector to rapidly gain military cyber resilience
  - *Survive:* Apply legacy hardening and resilience moves in the civilian sector to improve their posture
  - *Succeed:* Transition transformational systems to critical infrastructure and the civilian sector

Strategic Context

- ***Risks:*** Adversaries exploit vast societal vulnerabilities exposed via pervasive insecure ICT
  - Vast intelligence losses for US and allies
    - $3T in cyber-enabled IP theft against the US
    - Major weapons systems stolen (e.g., F35)
  - Deficit (crisis?) in military cyber resilience
    - Deterrence weakened
    - Warfighting capacities undermined
  - Destabilization of international security architectures
    - Crisis instability
    - Insecurity dilemmas
    - Misperception and miscalculation
- ***Strategic Impact:*** Adversaries are changing the distribution of technology, wealth, and power
  - *Interaction Framework:* action possibilities and payoffs for actors
  - *Meta-power:* Actions that change the distribution of action possibilities and payoffs
- ***Solution:*** USG must undertake a Cyber Blitz (Studeman) necessary to improve the US position at scale with speed
  - USG must implement an industrial strategy (long-, medium-, and short-term)
    - Overcome public goods dilemmas in security arising from market failures
    - Identify and exploit high-leverage technologies and frameworks
  - USG must catalyze a transformation of the ICT technology plane
    - The private sector must raise security and resilience on a prioritized basis
    - The security research community must fuel the blitz with new technical architectures and supporting metrics (retrodictive and predictive) that are work-factor aware

Dimensions of Multi-level Cyber Conflict: Information operations target societal systems by reaching through the cyber substrate

Dimension	No	Layers	Below LOAC	Description
Ideation	9	Socio-cultural	Yes	Ideation, value systems, cultural dynamics, Internet ecumene.
	8	Political	Yes	Political dynamics; ideology; political systems; legal systems; international governance; human rights; information control.
Policing	5	Criminality	Yes	International law enforcement cooperation, domestic law enforcement, criminal investigations, anti-crime efforts.
Security	7	Intelligence	Yes	Espionage, counter-intelligence, cyber defense; counter-terrorism; counter-influence.
	6	Military	Yes (Gray Zone); **No**	Inter-state cooperation & competition; balance of power; alliances; sovereignty; domains of land, sea, air, space, cyber; cyber defense & offense; information operations; defense industrial base.
Economics	4	Critical Infrastructure	**No** (at scale)	Finance, telecom, energy.
	3	Economic	Yes	Systemic stability, exchange rates, finance, trade, portfolio & direct investment, globalization.
	2	Technology	Yes	Operational technologies; standards and practices in communications, computation and cryptography.
	1	Science & Engineering	Yes	Research and development, especially ICT.

Multi-spectrum Adversaries (MSA) Orchestrate a Range of Capabilities Against a Target

Modes of Multi-spectrum Cyber Operations

1. **Remote Access** – CNE, CNA 'hacking'
   - Penetration via network (moving from OS to apps)
   - Accessing backups
2. **Insiders** – Traditional agents, social engineering
   - Disgruntled, ideological, or compromised employees
   - Unwitting violation of security practices (compromised credentials)
   - Digital media insertion
3. **Supply Chain** – Technology influence, including crypto and PKI
   - Design of HW, SW, environments
   - Manufacturing
   - Delivery and installation
   - Operation and managed services
   - Upgrade and maintenance
4. **Leakage,** Crypto attacks - Signal processing, machine learning, big data
   - Side channels (e.g., differential power analysis) and covert channels
   - Cloud co-tenancy
   - RF/EM - Wireless
   - Digital wake outside IA defended zone

Principles of Information Assurance

- **Gosler's Law:** Adversarial threat is conserved across attack surfaces
  - Architectural change displaces preferred attack points
  - Move attack points to where they can be best defended
- **Markowitz's Law:** A minimal complexity system has fewer attack surfaces.
  - Eliminate unnecessary functionality
- **Architectural Leverage:** Effective security can be achieved through synergistic architectural moves targeting attacker work factor
  - Success is achieved by raising attacker work factor across attack surfaces beyond the resources available to the attacker, or worthy of the target
- **Low Diversity Risk:** Concentration of value attracts better resourced attackers whenever attacker work factors do not increase faster than the value at risk
  - Attackers can gain economies of scale through common mode vulnerability
  - Multiplexing functionality on a platform aggregates the separate threat models
- **Giorgio's Law:** Information sharing and preserving confidentiality are inversely correlated
  - Sharing (and mobility) multiplies attack surfaces!
  - Eliminate unnecessary sharing, use fine-grained control (e.g., security tagged architectures)

Cyber Risk Reduction

Risk = f	(Threat		Vulnerability		Consequences)	
Attacker	Intent	Capabilities	Inherent	Introduced	Fixable	Fatal
Defender	Deter	Disrupt	Defend	Detect	Restore	Discard
Strategy*	Shape Interactions		*Increase Assurance*		*Increase Resilience*	
Deterrence*	Punishment		Denial		Denial/Entanglement	
Norms*	Stability Measures		*Architectural Change*		*Duty to Assist*	
Trade*	Shape Interactions		*Industrial Policy*		*Industrial Policy*	
Visibility*	Illuminating Sources & Methods		*Map To Societal Functions*		*Map Critical Dependencies*	

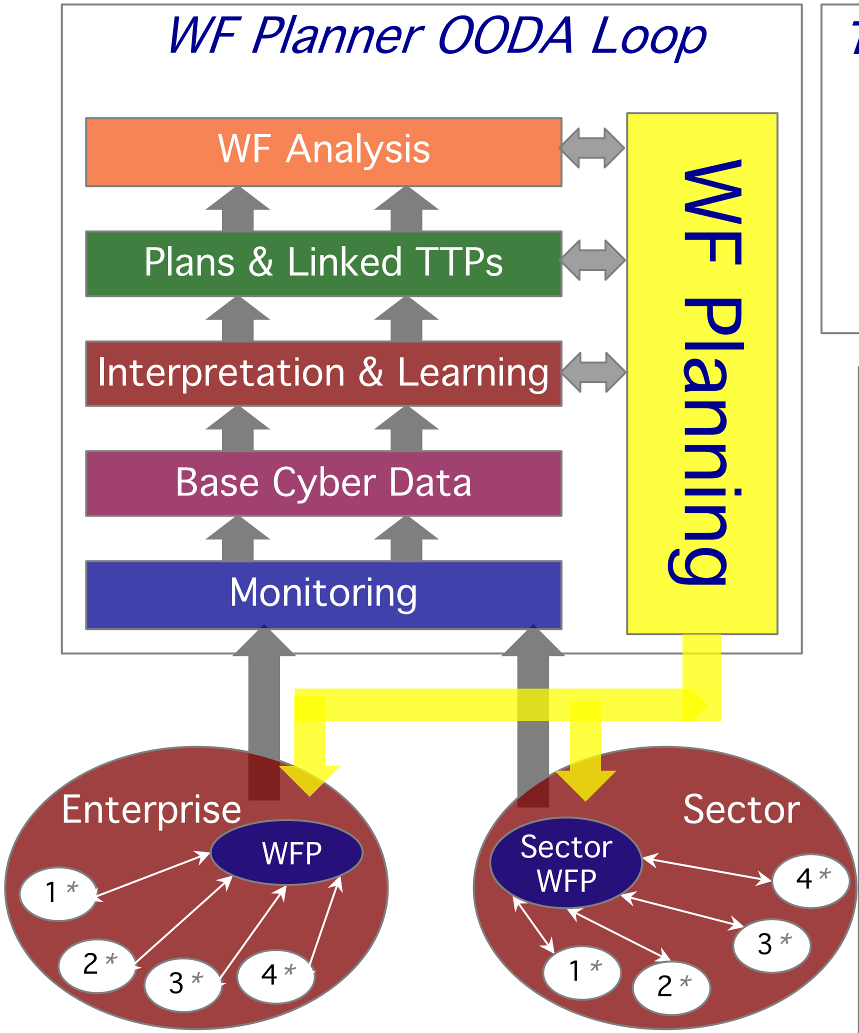
DSB Layered approach for managing cyber risk:

- When properly executed, defensive strategies can defend against Tier 1 and 2 threats.
- Defending against known vulnerabilities is an insufficient strategy against Tier 3-4 threats.
- Since it will be impossible to fully defend our systems against Tier 5-6 threats, deterrence must be an element of an overall risk reduction strategy. Additional measures are required, such as consequence management.

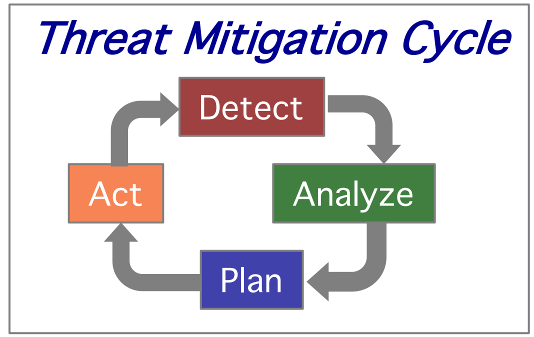
* *Mallery addition*

Source: Defense Science Board, *Resilient Military Systems and The Advanced Cyber Threat*, January 2013: 6.

Cyber Defense Work Factor Planner (WFP):
Operational Monitoring, Analysis, and Mitigation Planning Improves through Epistemic Refinement Loops

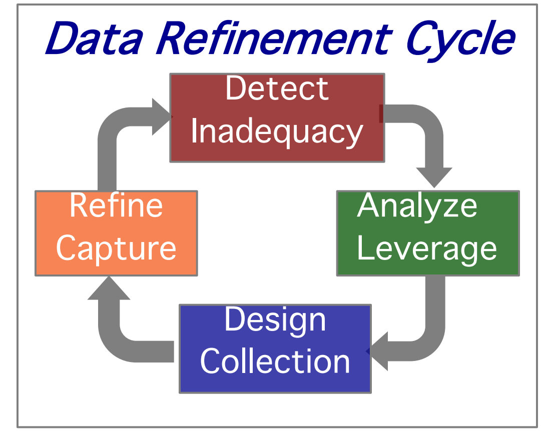


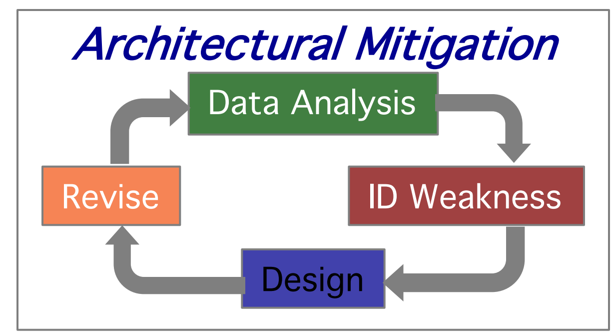
* Components

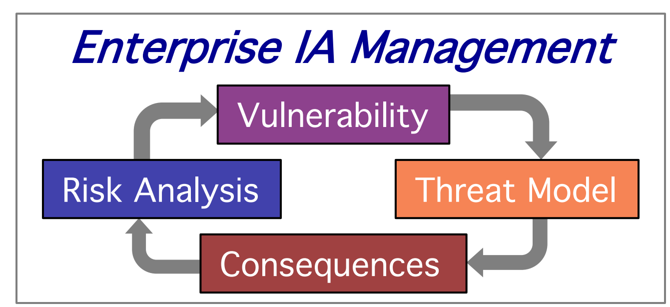


Data Types

- ✓ Indicators
- ✓ Incongruities
- ✓ Plans
- ✓ TTPs
- ✓ Lifecycles
- ✓ Attack graphs
- ✓ Defense graphs
- ✓ Threat Intel
- ✓ Targets
- ✓ Remediations
- ✓ Best practices
- ✓ Configurations
- ✓ OP procedures
- ✓ Architectures
- ✓ Strategies







Raise The Information Assurance Across Globalized ICT To Obsolesce Offensive Techniques and Moderate Cyber Insecurity Dilemmas

- *Technology Norm:* Raise the assurance level to implement , *ergo* deterrence by denial
  - Arms control = foregoing offensive capabilities
  - Cyber arms control = Shift the balance in favor of defense
    - Constrains opportunities for offensive cyber operations
- *Problem:* State restraint is imperfect
  - Cyber weapons are "covert capability"
  - Inspection and verification are unlikely
  - Enforcement is impractical
  - Law-following states are penalized
- *Approach:*
  - **Enhance security & resilience for military & civilian systems**
    - Increase survivability -> increase predictability for military cyber stability
  - **Prioritize based on criticality and downstream market scope**
  - **Phased implementation**
    - Target architectural changes to retire broad spectrum vulnerabilities
- *Benefits:*
  - Verifiable and enforceable raising of the costs to cyber operations
  - Move from *reactive* incident response towards *proactive* architectural change
  - **Address public goods dilemma (macro-micro problem)**
  - **Gain leverage to impact ~$4.3T annual sales of ICT products**
  - Moderate cyber insecurity dilemmas (Mallery, 2018a).

International Vulnerabilities Equities Process (IVEP)

Precedents

- *US Vulnerabilities Equities Process*
  - Published 2008, revised 2014, 2017
- Decision to disclose vs. retain vulnerabilities

What is IVEP?

- Identify high risk flaws:
  - Report significant cyber vulnerabilities and **architectural flaws**
  - Perform security analysis
- Short-term:
  - Enable rapid patching of critical vulnerabilities
  - Undermine attacker TTPs
- Medium-term:
  - **Incentivize industry to fix flawed architectures**

Who implements security fixes?

- Private sector

What are the targets:

- Critical vulnerabilities
- Broad spectrum vulnerabilities
- Key enablers for cyber arsenals

What actors execute IVEP?

1. ***Report:*** Governments, industry, academia report high risk flaws
2. ***Analyze:*** Technical experts perform security analyses
3. ***Incentivize:*** Industry, governments, and international organizations implement policies to incentivize fixes

What are the organizational modes?

1. ***Distributed:*** Entities operate independently and interact with each other as appropriate
2. ***Coordinated:*** Central institution(s) coordinate archiving, analysis, and/or implementation
3. ***Group Options:*** Small group, collective defense organization, trade groups (e.g., WTO), or UN
4. ***Membership:*** Governments, industry sectors, open source communities