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

John C. Mallery, WFA Group, LLC

jcma@mit.edu

BLUF: Overcome cyber security public goods dilemmas in information & communications technologies (ICT) by orchestrating policy levers to drive better information assurance and resilience based on a strategy grounded in work factor metrics as part of a cyber blitz.

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
- **Markets 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  - Outdated architectures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

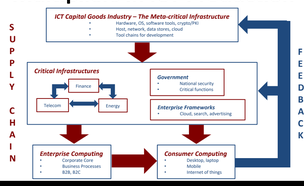
Technical Shortcomings

- Lack of memory safety
- Unmanageable complexity
  - Poor architectures fail to optimize locality
- Lack of total system security framework
  - Multi-spectrum attacker
  - 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 characteristics
    - Retrodictive and predictive metrics
  - *Return on Investment (ROI):* Ability of buyers of IT to reliably understand & measure risk
    - Anticipate 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
    - Architect for adaptive resilience and rapid recovery
    - Radically increase productivity of secure system development, certification, accreditation, and operation
  - *Realign Incentives:* Alignment of market incentives for uptake – ultimately next gen COTS

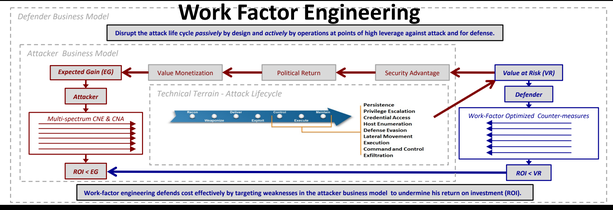
Multipliers In ICT Production



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 mean-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**
  - *Defense in Security Engineering:* System, platform, enterprise
  - *Depth: Early warning, Monitoring, Intervention, Learning*
- ***Cyber resilience engineering uses*** **work factor analysis to compare attack/defense difficulty across modes of recovery**
  - Intelligent adversaries move to the weakest attack surface
  - Minimize structure/resource sharing across attacker plans

Work Factor Engineering



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

- Cyber Solarium Commission Recommendation
  - National Cybersecurity Certification and Labeling Authority (Reccommendation 4.1)
- NIST Cybersecurity Labeling Program
  - May 2021 Executive Order 14028 requires consumer labeling for Internet of Things products (IoT) and 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

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

15 Policy Levers for Incentivizing Better Assurance and Resilience

National

1. Federal R&D & Procurement
2. Name and Shame
3. Indirect Incentives via Best Practices
4. Insurance Markets
5. Tax Policy
6. Legal Responsibility
7. Direct Regulation

International

8. Trade Incentives
9. Major Vendor Unilateral Action
10. Industry Standards for Products and Services
11. Voluntary Accords for Sectors
12. Technology Norms
13. National Regulation based on Standards
14. Policies of Supranational Entities and Alliances
15. World Trade Organization (WTO)

Policy: Prioritize Efforts to Achieve Work Factor Impact on Adversaries

1. *Cyber Blitz:* Execute strategies that define actual paths to success (Adm. (ret) William O. Studeman)
2. *Research:* Fund R&D programs to develop game-changing ICT
   - Work Factor Engineering
   - *Security:* Information flow control in the enterprise
   - *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
   - 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

C3E

Computational Cybersecurity in Compromised Environments

2021 Fall Workshop | October 27-28 | Virtual