Reversing Cyber Risk Assessments for High-Value Returns

Brian Mork, Ph.D., Col USAFR
AFRL/XPZ Senior Plans & Programs Engineer
Brian.mork.1@ usaf.af.mil.
937-904-8400
Rev 2018.3.5

…showcase **current research**, new tools and techniques, **leading edge procedures and processes**, best-in-class practices, and **perspectives of representatives from** academia, industry, **DoD**, and other government agencies on timely, relevant, and **emerging topics** critical to the future of the test and evaluation.

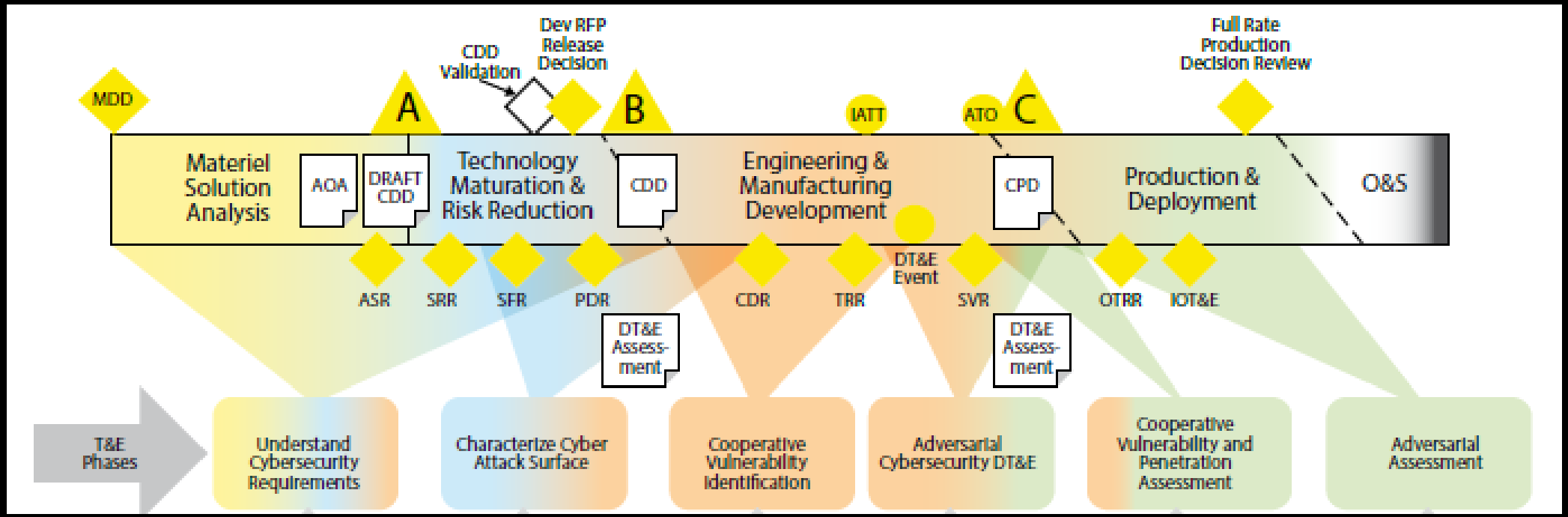
Outline

- Mission/Cyber vs. Cyber/Mission
- Engineering Intent method
- Three Perspectives:

  Risk Lexicon, New Paradigms, Discovery
- Program Management implications
- Cyber method maturation time line

The views expressed herein are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or U.S. Government.

DoD Cybersecurity T&E Guidebook



Advocates a 6 Phase process …iterative.
…recursive.
…repetitive.

Complicated for a PM

Lots of Methods

Authorities flow down for the Air Force:

- Task Force Cyber Secure (CSAF Mar 2015)
- Cyber Resiliency Steering Group (8 commands/centers, 2015)
- NDAA 2016 Cyber Campaign Plan 7 LOAs (AFMC & AFSPC Sep 2016)
- **C**yber **R**esiliency **o**f **W**eapon **S**ystems CROWS (SES)
- PMs, researchers, designers, buyers, operators

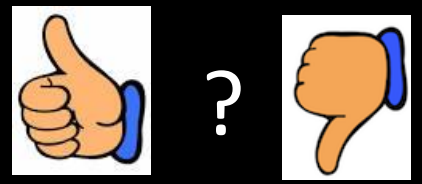
DASD(T&E) Summer 017.

- PMs need help – compared 20+ methods.
- Recommendation: start with **C**yber **T**able **T**ops.
- Mid-2017: 5 CTTs, 227 facilitators trained.

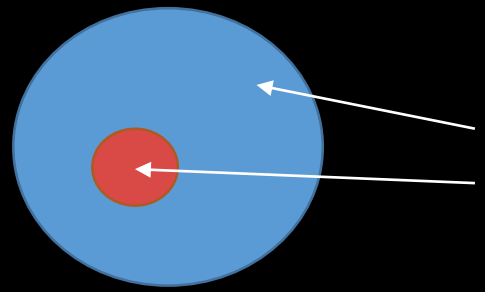
AFRL/RI → AFOTEC.

- Assessments driven by NDAA 2016 Para 1647. Productive Effort.
- Blue Books mid-2017: 31 systems, 45 by end of 2019.

Prioritize cooperative mission self-study.



Mission First Method

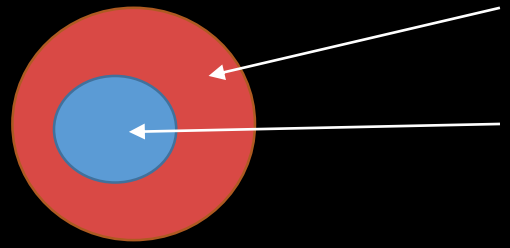


1. Design a military system
2. Mission team study
3. Publish self-knowledge of vulnerabilities
4. Cyber team confirms viability/access
5. Fix accessible vulnerabilities

- Mission-centric marginalizes Cyber red team - “Optional step of red teaming serves to satisfy the misplaced belief in the usefulness of red team assessment of mission assurance.”
- Assumes no vulnerability found by mission team indicates there is no vulnerability and therefore no threat.

  “If we don’t know about it, it can’t hurt us.”
- Defines away critical cyber threats such as zero-days unknown by both sides at present
- Finds extra things we don’t care about (mission damage that is not really doable)
- “Mission Assurance” normalizes equipment failure: similar to transport pilot MEL

Alternative: Cyber First Method

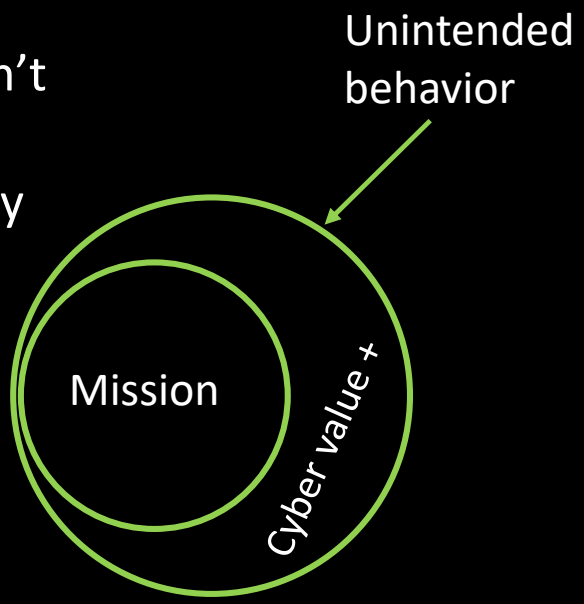


1. Design a military system
2. Cyber team discovery and research
3. Publish behavior contrary to design intent
4. Mission team prioritizes impact
5. Fix design/use mistakes and risk

- Cyber team acts as dynamic Aggressor, not static Threat Surrogate
- Find behavioral deviation from the engineer's intent
- Real threat is what both sides don't yet know – goal: find it first!
- BTW – periphery is useful to others: Ops, Mx, Logistics, DOTMLPF

Engineering Intent Method

- Engineering Intent Method – to assess <u>and</u> influence design to “bake in”
  - Attention on the “box and binary”
  - Recognizes cyber is in the delta, two types: box v. docs, good guy v. bad guy
  - Provides a path to “baked in” security rather than just mitigation
  - System stability ensures mission assurance
  - <u>Assessments</u> are for legacy. E.g. OT&E vulnerabilities per NDAA 2016. Don’t be distracted.
  - <u>Design Resilience</u> for the future. E.g.? blockchain the fleet; crowd integrity



RISK is best built on 3 pillars

Who Owns?	Risk Pillars	AFRL/RY HowTo *	Resiliency Tenets *
Acquisitions	Vulnerability	Reduce Susceptibility	Move out of band
Adversary	Threat	Deny Capability	Detect, React, Adapt
Operator	Impact	Reduce Access	Assure critical missions

1. Convoluting vulnerability and threat understates risk. *Risk is more than this*.
    1. 2002 confusing NIST definition "Threat is potential of a threat source to exercise vulnerability"
    2. "If there is no vulnerability, then there is no threat". Empirical Aristotle does not imply Ontological Plato.

2. Defining vulnerability as susceptibility + threat (cap + access), overstates risk. *Risk is less than this*.
    1. Every design is *susceptible* given time and desire; "I exist, therefore I'm susceptible."

3. NIST 800-30 Rev 1 changed away from VA to RA. VA is removed from table of contents. Massive rewrite. If you're doing only vulnerability assessments, you're missing 2/3 of the problem.

* From Hughes & Cybenko, 2013

New Test Paradigms for Cyber

RED TEAM

- Old: Mimic the adversary. Power is proportional to cyber knowledge.
- New: Like an adversary, discover techniques. Power is $\frac{\partial cyber}{\partial t}$.
- E.g. NASIC **S**ystem **T**hreat **A**nalysis **R**eports -> **V**alidated **O**nline **L**ifecycle **T**hreat

TEST DATA - for a PM to make decisions

- “Somebody”, “somewhere”, “under the right circumstances” can compromise your system. PM has to balance tech risk, cost, schedule!
- Radar analogy – mature math beyond binary “we did/not detect it” Test data is probabilistic analog estimates with confidence intervals.
- Metrics for now: “No Engineering Units” - Relative improvements.

Self-Knowledge vs. Discovery

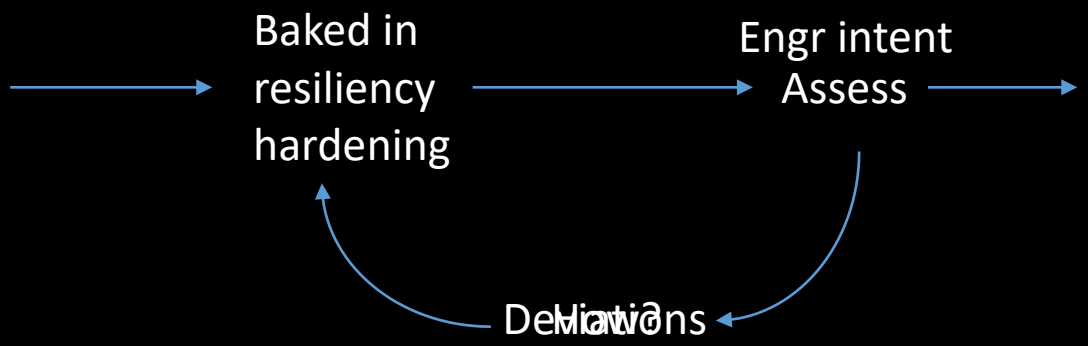
- Character of cyber is discovery, not just confirming design documentation.
  e.g. Fuzzing keyboards – 100% of design requirements are met, and still a problem.
- Examples show designs are not bad or negligent, just insufficient for the future.
  WAP, WPA2, Bluetooth, CPU speculative execution…
- Info Exchange Boundary scopes the problem for certain assessment types
  …and prevents seeing the entire landscape – adversary is looking wider.
  e.g. Does a Mission team CTT consider the compiler as a mission impact access point?
- Pursue cyber like a tracker, don't set boundary markers like a surveyor. Cyber power is resident where you don't survey.

January 2018

"Meltdown and Spectre are examples of what happens when we reason about security with abstraction (*a.k.a. requirements and documentation*), and then encounter minor discrepancies between the abstraction and reality."

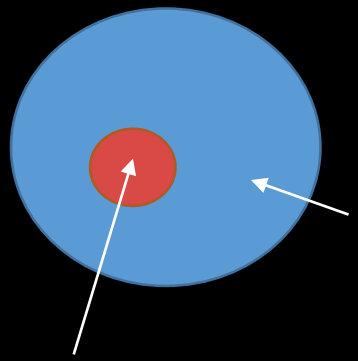
Program Management Ideas

- Cyber assessment shouldn't duplicate System Engineering
- Cooperative assessment vs. non-cooperative discovery: cost and schedule.
- Skillset – NSA approved, AFSPC approved training. IOC when? Authority to connect?
- Retention issues of military. Using experts in industry ends with SETA or TSPR.
- DoD Cyber T&E process – presently without design feedback. When? How?
- If wait for production boxes and binaries (MS-C), we're patching, not baking in.
- Safety team analogy to CTT – but safety has no bad-guy (enemy gets to vote).
- Un-prioritized info is not much better than none
- Alternative – civilian warriors. Examples – ARC WEPTAC. AFOTEC. Proper 3rd party perspective and still mission savvy.



Cyber Risk Method Matures by Reversing

NDAA 2016, Section 1647
"Thou shalt" (forces fast and low cost)

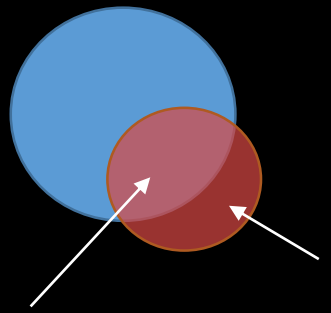


"Chicken Little"
(chaff to the PM)
Duplicates SE

Mission relevant cyber attacks

- DOD T&E 6 Phase
- Cyber Aggressors

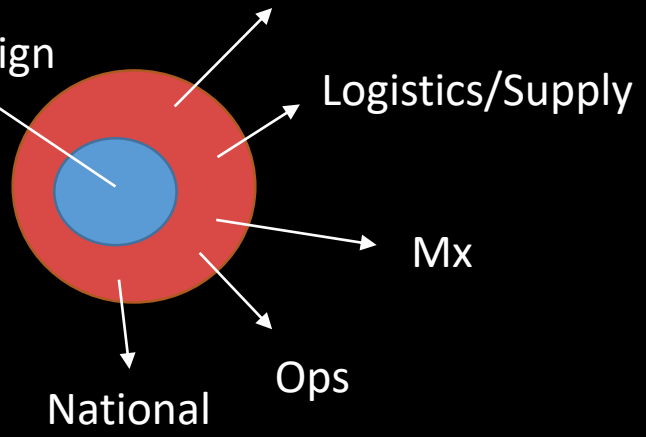
(hybrid process 2016-2019)



e.g. APTs, Exfiltration

e.g. IADS corruptions

Engineering Deviations
2020 -



= Blue Team Findings (mission)

= Red Team Findings (technique viability)

Conclusions

- Cyber is in your differential, and their differential. Kinetic. Dynamic. $P \propto \frac{\partial cyber}{\partial t}$.
- Stand on the 3-legged stool for common language.
- Current land-scape of assessments is sufficient to answer NDAA 2016 and AF CCP “mitigate”.
- Current land-scape of assessments does not answer AF CCP “bake in” cyber resiliency.
- Red team discovery efforts are more elucidating than being an intel surrogate.
- Reverse the process and do cyber aggressor discovery before mission analysis.
- Maybe skilled military aren’t retainable. Leverage Total Force move to “vernier” soldiers.
- Engineering deviation assessment methods reduce downsides and add value.

Reversing Cyber Risk Assessments for High-Value Returns

Feedback to:

Brian Mork, Ph.D., Col USAFR
Brian.mork.1@ usaf.af.mil.
937-904-8400