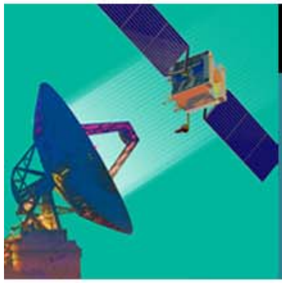
Working Group Outbrief

Ground System Architectures Workshop

Session 11E

Achieving Cyber Resilience in a Budget Constrained World

Frank Belz, Marybeth Panock, The Aerospace Corporation



Context of the Working Group

Mission success in space will increasingly depend upon mission resilience in the presence of attacks conducted in whole or in part in Cyberspace. Such attacks are likely to exploit weaknesses in the ground systems for space missions. The longstanding focus on preventative information assurance has shifted toward achieving cyber resilience of space systems and missions.

The funds available to address these new challenges are expected to be in ever shorter supply. As a result, there has already been an increased emphasis on exploitation of multi-mission ground resources to achieve mission operations, including for example, migration to enterprise private cloud infrastructures. Such a migration introduces a whole new context for understanding what to do to achieve system and mission resilience.

Session Goals

- **Explore the challenges associated with pursuing Space Ground System cyber and mission resilience at a time of budget draw downs**
- **Engage the wisdom and experience of our panel of experts (and all participants) to better understand, e.g.,**
  - **How to prioritize IA and Cyber functions and procedures?**
  - **How to adapt throughout the lifecycle?**
  - **Where will re-invention be possible and/or necessary?**
- **Learn about activities being conducted by the panelists and participants**

Presenters/Panelists

Panelists

- **Lt. Col. Jeff Gray,** USAF Space and Missile Systems Center
- **Mr. Liam O Murchu,** Symantec

Key Points

- Decreasing budgets forces you to keep your eye on the ball
- We live in an entitlement culture – we throw away bits because we can – this creates opportunities for attackers
- Cyber defenders need to train like you fight
- Integrate cyber defense with operational system
  - Need to run cyber capabilities under operational conditions
- Need to understand nominal behaviors so that off-nominal indicators can be recognized
  - But sophisticated threats learn to hide in the noise / fly under radar
- Getting the right skilled people in the right place is key to resilience – scarce and not cheap

Key Points (cont.)

- Do need to share information for national defense
  - Sharing info enhances decision maker’s ability
  - But don’t need to control NSS satellites with our iPhones
- Do need to protect integrity of mission critical info
  - But need to triage so that less critical functions and data may be isolated or sacrificed
    - to reduce threat surface and
    - preserve most critical functions and information
- Key challenge – making the network defender knowledgeable enough to make the right decisions
  - 22 year old needs direction ahead of time to know what to isolate / shut down first in the heat of cyber battle
  - And what to bring back up first

Key Points (cont.)

- High level methodologies are emerging to prioritize among multitude IA and Cyber functions and procedures
  - Devil is in the details – every mission and system is different
  - Key is to get the right stakeholders engaged
    - Mission owners
    - IA
    - NW defenders
    - System engineers
    - Sys Admins
    - Program protection people
    - …

Conclusions

- Doing the basics (installing security software, maintaining, configuring, …) does protect against ordinary attacks
- Advanced persistent threats require significant investment
- There are things that can be done to improve cyber resilience in a budget constrained environment
  - Go for non-materiel solutions before spending development dollars
  - Know who the cyber defenders are
  - Understand your network, its interfaces, how it behaves and what data it carries
  - Understand how to triage mission functions
  - Plan for incident response

Back Up Charts

- Additional Points raised during the discussion
- Working Group Agenda
- Questions used to stimulate the discussion

Additional Points

- Linkage of space operations and cyber operations
  - Essential for mission
  - Creates tensions. Example:
    - Space Ops – high reliability, no planned downtime
    - But comm networks generally do have planned downtimes
- Necessary to understand true minimal level of capability
  - Below which no longer can serve the mission
- Existing programs may not have cyber requirements
  - Cyber requirements are prerequisite to design system engineering trades that include ability to respond to cyber threats
  - But cyber threats may be present anyway

Additional Points (Cont.)

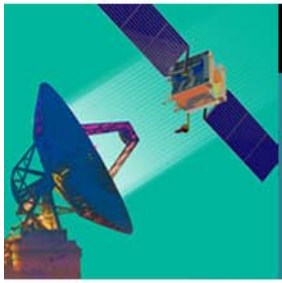
- People are key to improving resilience even with reduced budget
  - People who know what to expect, what is happening, and what to do are critical
  - People untrained / inexperienced in operational environment won’t be able to use high tech expensive tools
- Knowing the actual network and its boundaries is perpetually necessary
  - Topology and boundaries changing all the time
  - Baseline architecture documentation must be up to date

Additional Points (Cont.)

- In a simpler world, problems were also simpler
  - – New systems more complex
  - – Net-centricity leads to additional complexity
  - – Question: Is the current level of complexity really necessary?
  - – Answer:
    - Systems do more and commanders need more
    - Do need to share information for national defense
      - – Sharing info enhances decision maker’s ability
      - – But don’t need to control NSS satellites with our iPhones

Additional Points (Cont.)

- Decision processes (both in development and operation) are what need to be improved
  - Understanding facts that are required to know what to do
  - Strategies and tactics for decision-making must be informed
  - Prioritization is critical
    - E.g., system simply will not operate if <conditions> hold
  - Continuous situation understanding / adaptation essential for both prioritization and decision making
  - In cyber, essential to have rapid ability to simplify / triage both systems and operations
    - Preworked triage structure (possibly with local ad hoc refinements)



Additional Points (Cont.)

- Even turning off system / devices won’t guarantee security
  - Remote activation of mobile devices is usually enabled
- Consider that a mission’s different operational modes may require different responses to ambiguous anomalies
  - Approach when known to be under attack may be faster, more radical to preserve essential functions
  - Transition to higher threat modes may require collaborative situation awareness

Additional Points (Cont.)

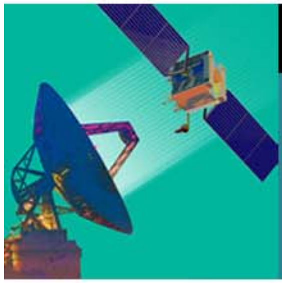
- In a system-of-systems environment
  - Mutual mission dependencies may not be obvious
  - Pre-working decision options, triggers may be essential
  - Cyber "safe modes" must be pre-defined for rapid recovery
  - (Re)planning and (re)training under operational conditions becomes essential
- May not know about dependencies until someone "pulls the plug"
  - Consider pulling the plug in operational exercises (not just military game environments)
    - Systems and people must respond: training moments occur
  - Netflicks' "Simian Army" approach is application of this approach randomly, even during peak business hours

Additional Points (Cont.)

- Must operate space systems with cyber capabilities ON
  - Overcome desire to run with cyber capabilities OFF to not degrade performance
  - It is not just the technology, but the people and processes that must be considered by engineers
- Claim: More controls (in sense of DoD 8500 or NIST 800-53) mean better assessment
  - Counterclaim: In DoD, more controls mean more controls, more cost, more complexity
  - Again, how to prioritize?

Additional Points (Cont.)

- OSD push for improved program protection planning could be a step toward cyber resilience
  - Need protection plan AND IA defenders AND sustained availability: a sweet spot
  - What is really important may not be what is shiny and new (and expensive)
  - Sometimes people bring vulnerabilities to the system due to OPSEC lapses
    - E.g. wireless devices (cellphones, etc.) in restricted areas
  - Computer Network Defense is way more than compliance with controls
    - It is about defending your assets

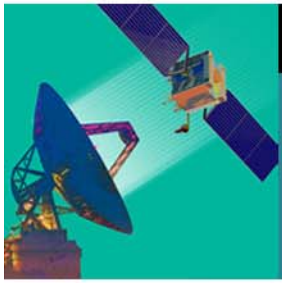


Additional Points (Cont.)

- Challenge: be prepared for adversary who has honed its skills in the “Cyber Arms Race” we see on the Internet
  - Important to add an analysis arm to the Cyber Defense team
    - Invest in tools, people
    - Even one more person on the team focused on forensics (with good tools) can make a big (and critical) difference
      - But hard to find these people
- On the difficulty of attribution (to the responsible party in the case of an attack)
  - Privacy concerns make attribution more difficult
  - Anonymity prevents attribution

Additional Points (Cont.)

- Resilience may depend on swiftness of counter actions and consequences – deterrence may depend on attribution
- Espionage may be harder than sabotage



Additional Points (Cont.)

- Incidence response is when the security team is noticed
  - Need plans, policies, procedures in place, well-organized team
  - Need to discover you are IN an incident ASAP
  - Data capture critical to forensics
- Hi-value targets
  - Demand better protection as part of resilience
- Predominant motivation of threat actors has matured
  - Fame -> Money -> Political agenda (hactivist, …)
  - Well funded, skilled attackers increasingly impactful
- Most attacks in industry are not sophisticated

Additional Points (Cont.)

- For every mission, the process comes down to risk assessment, mitigation, management
  - As attacks move from espionage to sabotage, thinking changes
    - Need for protection increases
    - Need for resilience increases
    - Willingness to invest in technologies, operational change, training all goes up
- We are beginning to see a convergence of the perspectives in commercial IT industry and National Security Space
  - But more money to attract better people in commercial sector

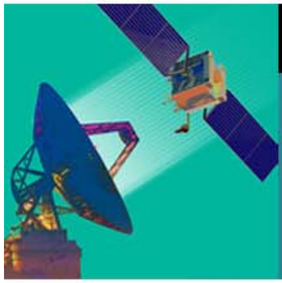
Working Group Agenda

1:00	**Introduction by Session Co-Chairs**
1:15	**Introductory statements from the panelists**
1:45	**Extended exploration of achieving ground system cyber resilience in a budget constrained world, focusing on the challenges we face and opportunities we have** ***Panelists and all participants will engage in responding to provocative questions and will formulate their own…***
3:00	**Break**
3:15	**Continued exploration**
4:45	**Recap of most important observations and insights of the day**

Discussion Questions

1. Hypothesis: *The starting point for this working group is the assumption that it is possible to improve the resilience of space missions to cyber attacks, even while budgets for space system development / enhancement / maintenance are decreasing.*

- Questions:
  a. Do you believe it is (or is not) possible to improve the resilience of space missions to cyber attacks while budgets are decreasing?
  b. What evidence would you use to support your position?
  c. What factors do you think are in play in your assessment of this hypothesis?
  d. Where are the biggest or most critical gains possible (or necessary)?



Discussion Questions (cont.)

3. Observation: *It is often observed that constraints inspire creativity. If the obvious way to "get a job done" is out of the question, creative humans have often been able to innovate entirely new ways to get the job done – **if** the will to get the job done is high enough.*

- Questions:
  a. To what extent or in what ways do you think the challenge of cyber resilience can/will stimulate or even force creative solutions?
  b. Do we even need creative solutions? Are there obvious, simple ways to address achieving cyber resilience in an increasingly cost constrained world?

Discussion Questions (cont.)

1. Hypothesis: *The starting point for this working group is the assumption that it is possible to improve the resilience of space missions to cyber attacks, even while budgets for space system development / enhancement / maintenance are decreasing.*

- Questions:
  - e. Do you believe the challenge we face to improve space mission resilience is the subject of a zero-sum game – e.g., there is only a certain amount of money available to develop and conduct a space mission, and investments to achieve mission resiliency will require reductions of expenditures to achieve other important mission achievements?
  - f. What evidence would you use to support your position?
  - g. Specifically consider this possibility: Might increased resilience reduce costs? – how?

Discussion Questions (cont.)

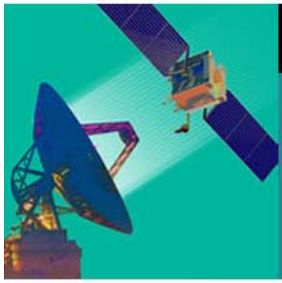
2. Observation: *Reduced budgets may impact both the development of space systems (including for example satellite ground systems) and their operation. The factors governing which part of the overall lifecycle will be most impacted are not yet clear (at least to us).*

- Questions:
  a. If mitigating risk to mission resilience is a high priority, is there a rational approach to deciding where to focus budget cuts and where to maintain or enhance investments?
  b. For example, in the near term, to what extent and in what ways could increased investment in development not only reduce risk in operation but also life cycle cost of the system?

Discussion Questions (cont.)

4. Observation: *The nature of commodity cyber attacks has been changing for the last few years significantly. At the highest level, many entries are being attempted using social engineering such as phishing attacks. Within the boundaries of cyberspace, innovative ways to bridge air-gaps have been seen.*

- Questions:
  a. From your perspective, based on recent history, how do you see the near future of cyber engagements in the commodity Internet world?
  b. If satellite/space ground systems use commodity network technologies, host computers, and commercial software (which they do), what should the experience in the Internet cyber “wild wild web” be teaching us about the ground system cyber challenges?



Discussion Questions (cont.)

5. Observation: *Mission cyber resilience is required during the operations phase of the lifecycle. But the ability to be resilient depends upon preparations made before and throughout operations. This involves not only the space system including the space ground system, but also operational procedures, organizational structure, training, and continuous monitoring / testing.*

- Questions:
  a. How should one select and prioritize among IA and Cyber functions and procedures (think, for example, of the 800-53 controls) for achieving resilience in the presence of cyber attacks?
  b. What must be done to achieve adaptability to the changing threat vectors of cyber attacks?
  c. Where will re-invention be possible? Necessary?

Discussion Questions (cont.)

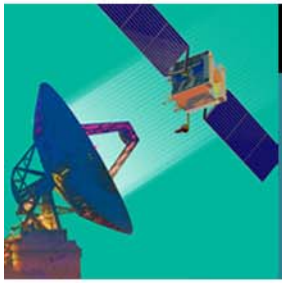
6. Observation: *To a certain extent space ground systems resemble industrial control systems (ICS) and physical process supervisory control and data acquisition (SCADA) systems.*

- Question:
  a. What can we learn from Stuxnet, its successors, and other ICS/SCADA attacks that would apply to space systems?

Discussion Questions (cont.)

7. Observation: *If we consider a conventional stack of capabilities, resembling the OSI 7-level stack model, threat vectors can be executed by way of any and all layers. At the top are human users. At the bottom are physical communication media. In the middle are applications, middleware, host operating systems, and complex networking and internetworking capabilities. Overlaying this stack are sensing, control and management functions that are used to observe, control, and manage the behavior of the entire system and its interfaces with other systems. Over the last few decades in the wild wild web, the center of attention (of threats and countermeasures) has been shifting to the upper levels of the stack.*

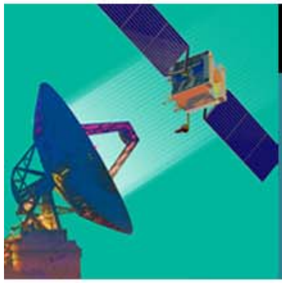
- Questions:
  - a. Consider each of these systems and communities that are part of an overall mission architecture. What constitutes success for their role in the preservation of mission resilience under cyber attack?
    - Mission operations centers.
    - Network (and Security) operations centers.
    - External / commercial security services that deal with commodity software and systems being used in the ground systems.
    - Government players, like NSA, AFSPC, SMC.



Discussion Questions (cont.)

7. Observation: *If we consider a conventional stack of capabilities, resembling the OSI 7-level stack model, threat vectors can be executed by way of any and all layers. At the top are human users. At the bottom are physical communication media. In the middle are applications, middleware, host operating systems, and complex networking and internetworking capabilities. Overlaying this stack are sensing, control and management functions that are used to observe, control, and manage the behavior of the entire system and its interfaces with other systems. Over the last few decades in the wild wild web, the center of attention (of threats and countermeasures) has been shifting to the upper levels of the stack.*

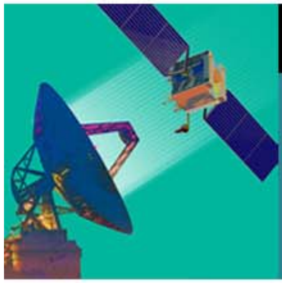
- Questions:
  b. Where among each of these are the greatest opportunities to improve our ability to establish and maintain mission resilience?
     - Mission operations centers.
     - Network (and Security) operations centers.
     - External / commercial security services that deal with commodity software and systems being used in the ground systems.
     - Government players, like NSA, AFSPC, SMC.



Discussion Questions (cont.)

7. Observation: *If we consider a conventional stack of capabilities, resembling the OSI 7-level stack model, threat vectors can be executed by way of any and all layers. At the top are human users. At the bottom are physical communication media. In the middle are applications, middleware, host operating systems, and complex networking and internetworking capabilities. Overlaying this stack are sensing, control and management functions that are used to observe, control, and manage the behavior of the entire system and its interfaces with other systems. Over the last few decades in the wild wild web, the center of attention (of threats and countermeasures) has been shifting to the upper levels of the stack.*

- Questions:
  c. Where among each of these are the greatest opportunities to reduce costs?
     - Mission operations centers.
     - Network (and Security) operations centers.
     - External / commercial security services that deal with commodity software and systems being used in the ground systems.
     - Government players, like NSA, AFSPC, SMC.



Discussion Questions (cont.)

7. Observation: *If we consider a conventional stack of capabilities, resembling the OSI 7-level stack model, threat vectors can be executed by way of any and all layers. At the top are human users. At the bottom are physical communication media. In the middle are applications, middleware, host operating systems, and complex networking and internetworking capabilities. Overlaying this stack are sensing, control and management functions that are used to observe, control, and manage the behavior of the entire system and its interfaces with other systems. Over the last few decades in the wild wild web, the center of attention (of threats and countermeasures) has been shifting to the upper levels of the stack.*

- Questions:
  - d. Comparing the greatest opportunities to reduce costs to the greatest opportunities to improve our ability to establish and maintain mission resilience….
    1. Is this a cause for despair?
    2. Hope?
    3. Both?