Securing Our Future in Space

Brig Gen (ret) Gregory J. Touhill, CISSP, CISM

Director, CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0539

Disclaimer

The views expressed are those of the presenter and do not necessarily represent the views of Carnegie Mellon University and the Software Engineering Institute.

The following thoughts and observations are based on decades of experience in the development, fielding, support, and operations of space-based military and civilian space capabilities supporting national security and national prosperity.

Acknowledgement

Thanks to my colleague, Chris Inacio, SEI/CERT Chief Engineer, for sharing his thoughts and experience in the development of space-based systems and specialized software supporting the space mission.

Security Controls Caution

While this slide deck is intentionally crafted to be UNCLASSIFIED, please be advised that the content of the delivered verbal briefing will likely include classified and controlled unclassified information. Please institute appropriate security controls for your notes.

My Perspective Influenced By My Experiences

Photo from *United States Air Force*. https://www.af.mil/About-Us/Biographies/Display/Article/108360/brigadier-general-gregory-j-touhill/

Today's Agenda

- Myth-Busting
- Understanding Threats and Risk Exposure
- Thinking Like Sun Tzu through a Hacker's Eyes
- Test & Evaluation as a Critical Risk Management Control
- Peering Beyond the Event Horizon

Myth Busting

Myth #1: Space Is a Safe Haven

For many years, the collective wisdom was that space was a safe haven.

- Adversaries could not equal our technical capabilities in space.
- RF/EM protection was relative to the perceived threat.
- Space-based and ground assets were “isolated and disconnected” from digital threats.
- Attacks against our space-based assets were extremely expensive and easily detectable and attributable.

Then Came the Land War in Europe

"Russian military reportedly hacked into European satellites at start of Ukraine war"

-- Corin Faife, *The Verge*

"Russia hacked an American satellite company one hour before the Ukraine invasion"

-- Patrick Howell O'Neill, *MIT Technology Review*

"Anonymous-linked group hacks Russian space research site, claims to leak mission files"

-- Corin Faife, *The Verge*

"Viasat shares details on KA-SAT satellite service cyberattack"

-- Sergiu Gatlan, *BleepingComputer*

Myth #2: We're Disconnected from the Internet

Our architecture is dedicated solely to us so only we have access to it.

- Our hardware is custom, mission-purpose gear.
- Our software is custom-built for the mission.
- Our ground segment uses dedicated lines.
- Our transmissions are protected by crypto.

Disconnected? Really?

"People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices"

-- Cybersecurity & Infrastructure Security Agency

"US: Chinese govt hackers breached telcos to snoop on network traffic"

-- Sergiu Gatlan, *BleepingComputer*

"It's important to know why things work on a star ship."

-- Admiral James T. Kirk

(Nicholas Meyer and James Horner. *Star Trek II, The Wrath of Khan*. USA, 1982.)

Myth #3: Redundancy = Resilience

One of the hallmarks of our space-based assets and architecture is the deliberate inclusion of redundant capabilities and controls.

- Redundancy has enabled spacecraft to operate well beyond their planned service lives.
- Redundancy has been focused on hardware; telecommunication; and telemetry, tracking, and control (TT&C).
- Historically, redundancy has yielded positive resilience results. Therefore, it is commonly assumed that it always will.

And Yet We Find Instances Where Redundancy ≠ Resiliency

We build flying science projects.

- Our sensors and radios are exquisite.
- The projects are cutting-edge, "just beyond proof-of-concept" efforts.
- The focus is on the hardware.
  - Second focus is the hardware.
  - Third focus is size, weight, and power (SWaP) (for the hardware, of course).
- Our satellites are very good, often working **well** beyond their design lifetimes.

"NASA lost its $125-million Mars Climate Orbiter because spacecraft engineers failed to convert from English to metric measurements when exchanging vital data before the craft was launched, space agency officials said Thursday."

-- Robert Lee Hotz. "Mars Probe Lost Due to Simple Math Error." *Los Angeles Times.* October 1, 1999. https://www.latimes.com/archives/la-xpm-1999-oct-01-mn-17288-story.html

Understanding Threats and Risk Exposure

The Touhill Cyber Threat Taxonomy

- Spies
  - nation state and industrial
- Burglars
  - financially motivated
- Muggers
  - take aggressive action to deter you from taking an action or to besmirch you
- Vandals
  - take action against you to impugn your reputation
- Saboteurs
  - often an insider, hostile actors who act to sabotage systems, processes, or mission
- The Careless, Negligent, Indifferent or Confounded
  - source of 95%+ of cyber incidents

Nation States and Cyber Outsourcing

Why build a cyber workforce when you can buy (rent?) one?

- Many nation states are hiring cyber criminals as 1099-like subcontractors.
- Incorporating lessons learned from cyber criminal group tactics, techniques and procedures (TTPs):
  - Specialists in certain cyber-operations capabilities are hired to perform discrete tasks as part of a carefully planned cyber mission operations team.
    - e.g., experts in cyber breaking and entering, database management, data science, applications specialists, networking, etc.
  - The mission team is created by the nation state mission manager, trains together for the specific mission, and then dissolves after the mission is closed.
- Some nation state actor personnel "moonlight" with cyber criminal groups to supplement their income.
  - Increases difficulty in attribution; proliferates nation-grade tools; quid pro quo benefits.

Nation State Space Motivations and Capabilities

Russia and China:

- Motivated by strategic national objectives and value superiority in space.
- Perceive US dependence in space as its Achilles' heel.
- Russia seeks to achieve "spectrum dominance" in "information confrontation." China has similar aims.
- They have "full spectrum" space capabilities, including directed energy weapons, tested anti-satellite capabilities and space-based weapons.

Iran and North Korea:

- Motivated by existential regime survival and actions that enhance regime legitimacy.
- Focus on counter-space capabilities against communications and navigation services.
- Conduct electronic warfare activities against adversaries.
- Can potentially use their developing missile and space lift capabilities to target orbiting satellites.

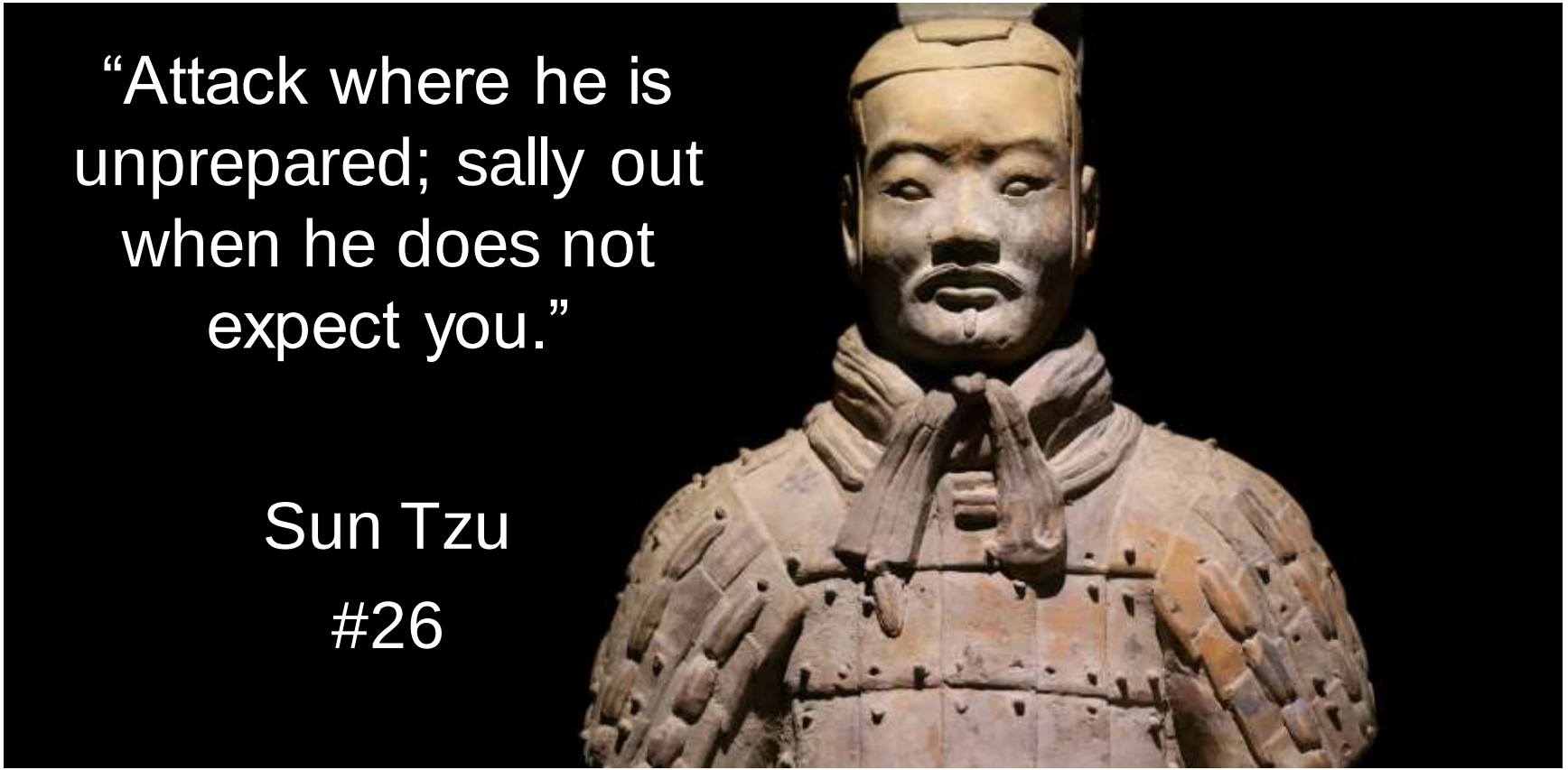
Reference: Defense Intelligence Agency. *Challenges to Security in Space (Unclassified)*. 2022. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

What's Our Risk Exposure?

- Cost, schedule, and performance is just a starting point.
- Risk surface to manage:
  - ✓ **Hardware**: we do well with custom-built, but not-so-much for off-the-shelf.
  - **Software**: always function-oriented; we've traditionally dismissed cyber threats.
  - **Wetware**: the human aspect of system design and risk management is often under-appreciated, under-measured, and uncontrolled.
  - **Third Party**:
    - with nation states: mostly focused on sharing of end products and disclosure
    - with vendors: transactional relationship with little independent, third-party auditing of security controls and posture
  - **Supply Chain**: Initially focused on hardware augmented by some situationally based background checks of personnel, much-needed efforts to improve supply chain risk management are underway

Thinking Like Sun Tzu through a Hacker's Eyes

Sun Tzu on War



Hackers on Cyber War

- “We put in the time to know that network. We put the time in to know it better than the people that designed it and the people that are securing it.” -- *Rob Joyce*
- “Social engineering has become about 75% of an average hacker’s toolkit and, for the most successful hackers, it reaches 90% or more.” -- *John McAfee*
- "Never Underestimate the Power of Stupid People in Large Groups.” -- *Hackajar*
- “Everybody is hackable. You’re going to get breached. It’s just a question of how quickly you can minimize the impact.” -- *Bryson Bort*
- “I get hired to hack into computers now and sometimes it’s actually easier than it was years ago.” -- *Kevin Mitnick*
- “The holes in a system have to fascinate you.” -- *Dave Aitel*
- “Never underestimate the determination of a kid who is time-rich and cash poor.” -- Cory Doctorow. *Little Brother, Tor Teen*. April 13, 2010. Page 87.
- “It is a fairly open secret that almost all systems can be hacked, somehow. It is a less spoken secret that such hacking has actually gone quite mainstream.” -- *Dan Kaminsky*

Some Hacker Acts While Thinking Like Sun Tzu

- Strategically looks for where you are “unprepared.”
- Does their homework on the target (i.e., you, your organization, your people).
  - Leverages open source and social media.
  - Determines your “blue order of battle.”
  - Understands your business, its organization and processes, and key personnel.
- Performs reconnaissance.
  - Scans your networks, looking for data such as:
    - known default passwords being employed (aka, a cyber “Kick Me” sign)
    - unpatched software and misconfigured systems
    - old, brittle, and easily exploitable systems and software
  - Identifies key privileged users and searches dark web and other data sources for compromised usernames and passwords that might be reused in the enterprise.
  - Conducts social engineering tests against your enterprise.

Questions You Should Be Asking

- Do we have a Zero Trust security strategy in place?
- Do our development personnel think like hackers? Do our security personnel?
- Do we perform reconnaissance against ourselves to look for the things that hackers look for to see where we are “unprepared”?
- Do we scan the dark web for indicators that our organization or our employees have been compromised?
- Do we invite others to help us identify where we are unprepared through bug bounties, red teaming, hunt teams, penetration teams, and other mechanisms?
- Do we conduct regular, independent, third-party audits of security protocols to assess our risk posture?
- Do we have the right technology, properly configured and operated, in place to offset human error?

Test & Evaluation as a Critical Risk Management Control

Test & Evaluation (T&E) Purpose

The fundamental purpose of T&E is to enable the DoD to acquire systems that support the warfighter in accomplishing their mission. To that end, T&E provides engineers and decision-makers with knowledge to assist in ***managing risks***; to measure technical progress; and to characterize operational effectiveness, operational suitability, interoperability, survivability (including cybersecurity), and lethality. This is done by planning and executing a robust and rigorous T&E program.

-- Department of Defense. *DoD Instruction 5000.80 Test and Evaluation*. November 19, 2020. Section 3.1.1. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF

The fundamental purpose of Test & Evaluation (T&E) is to provide knowledge to assist in ***Risk Management*** that's involved in developing, producing, operating, and sustaining systems and capabilities. The T&E process is an integral part of the Systems Engineering Process (SEP) which identifies levels of performance and assists the developer in correcting deficiencies.

-- *AcqNotes*. https://acqnotes.com/acqnote/careerfields/test-and-evaluation-overview

Test and Evaluation Realities

- Test and Evaluation (T&E) is a critical acquisition, due care, and due diligence function.
- We can't get security from T&E.
  - Bolting on security at the end is a losing game plan.
  - T&E's purpose is to ensure that sufficient controls in accordance with the requirements are in place to meet the designated mission.
- It doesn't solve the supply chain.
- It doesn't solve people or operations.
- We need strong and realistic threat models and capabilities to enable T&E to accurately test and evaluate against the operating environment.

What We Can Do to Help the T&E Process

We must have a solid plan to ensure the following:

- Our requirements and expectations are well defined and understandable.
  - Ensuring "cyber by design" and "cyber resiliency" are mission-critical requirements.
- Our architecture incorporates those "cybersecurity by design" and "cyber resiliency" requirements.
- We leverage a Zero Trust security strategy throughout the program of action.
  - Remember: Zero Trust is a strategy where "Zero Trust" is the starting point on the journey to "Digital Trust."
  - Our requirements need to define that "Digital Trust" model and criteria.
- Security microsegmentation controls that enable (and don't inhibit) the workforce.
- T&E has the tools and systems to accurately measure performance against requirements for all designated systems *and software*.

Peering Beyond the Event Horizon

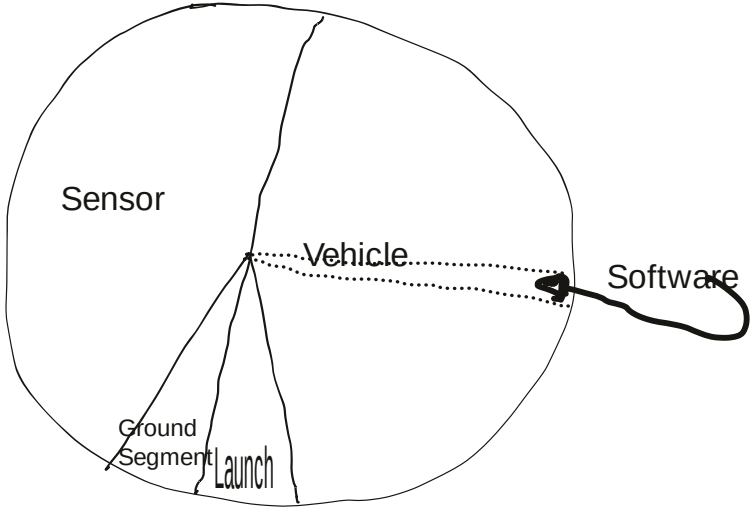
What Was Valid Yesterday May Not Be Tomorrow

- As we move to a more software-defined world and demand for dynamic retasking of mission capabilities increases, expect a greater investment in the production and controls of assured software.
- With higher demands made on software, expect commensurate demands on cybersecurity programs and activities through the lifecycle of programs.
- Systems engineering must incorporate software engineering, cybersecurity engineering, and artificial intelligence engineering to produce results that are effective, efficient, and secure.
- Test and evaluation activities will be performed much more often and earlier in the development of capabilities. Also, it will incorporate more automated tools to evolve T&E toward a more iterative process assisting leaders in detecting and measuring risks throughout the initial development process and throughout the lifecycle.
- Processing power requirements will drive an increased percentage of budget and engineering requirements.

So What's Changed?

- Adversarial capability has increased significantly.
  - There is no more safe haven.
  - Cyber is now a prevalent and increasingly potent threat in a multi-threat environment.
- There is a need for rapid capability delivery.
  - Given the "I want it now" generation, are traditional exquisite system engineering processes acceptable for the modern environment?
- Proliferation of LEO spacecraft
  - Ground segment might matter more here and may create a broader risk exposure.
- Advances in technology and coding make processing in space a viable and attractive option.
  - Maybe ground won't be as important - □□♂
  - AI and ML augmentation or replacement of crew? Processing in space!!!

Retrospective View of the Budget



After examining some satellite software and asking about some programs, this chart is the impression of the budget spend for a satellite project.

Source: Chris Inacio
SEI/CERT Chief Engineer

Putting Systems Engineering on Steroids

With greater reliance on software-defined mission sets, on-platform computing, deep space exploration, etc., complexity will increase, requiring enhanced systems engineering to orchestrate success.

- Detailed analysis of data paths and operational movement
- All data movement and error correction completely planned
- CPUs and busses sized to support mission, as bounded by communication- and sensor-driven function
- Data (usually fairly raw) sent to ground for processing

Software Becomes the Key Mission Enabler and Asymmetric Advantage

- Provisioning for “headroom in vehicle” capability to be flexible for planned as well as future processing needs is a high priority.
  - throughout development
  - after launch!!
- Constellations of capabilities and interactions
  - federated capability
  - distributed processing toward common objectives
- More open systems
  - higher bandwidth via a more open computer bus
  - more computational capability in vehicle
  - facilitates dynamic reprogramming and re-missioning ”on the fly”
- Faster, better, cheaper
  - including crypto!

What We Need to Do to Enable Software to Turn Science Fiction into Reality

- Leverage modern software engineering practices.
  - Plan, program, and budget for software commensurate with mission needs.
  - Ensure proper partitioning of software for space missions.
  - Allows risk isolation to enable rapid capability development and deployment.
- Take advantage of abundance of CPU cycles.
- Take advantage of abundance of memory.
- Optimize communications bandwidth.
- Incorporate DevSecOps into your development requirements and practices.
- And many more…

How to Enable Software

Make cyber assurance a mission-critical requirement.

- We need better space-rated crypto and should boost investments in this area.
- Invest in formally analyzed, highly assured OS and virtualization.
  - Must be instrumented for anomaly detection.
- Space scaled and sized container and virtualization solutions
- Hardware support for trust and isolation capabilities
- Supply chain, supply chain, supply chain
- Trust
  - Start with Zero Trust security strategy and architect trust deliberately.
  - requirements, hardware, software, wetware, policies, procedures, practices
- Secure every step of the way.
  - Insist on DevSecOps as a requirement.
    - DevOps (development AND operations) need to have security.

Shift Mindset from “an Exquisite Science Project” to a Rapid “Looks More Like an IT Solution”

- Still want and need exquisite sensing solutions.
  - ability to rapidly integrate them onto highly capable platforms
- Leverage constellation of capabilities.
  - performance
  - resilience
- Carefully considered trust design
  - Zero Trust is the starting point on the way to Digital Trust; it isn’t the destination.

Conclusion

Did I mention

Software?

Really, we're going to have to trust that we can do software to enable capability. We're really going to have to trust that we can build software processes to do this rapidly. And we're going to have to do cyber in a fundamentally more deliberate and rigorous way that spans across our requirements, hardware, software, wetware, etc.

We will make mistakes. We need trust roots, detection, crypto, and verifiable recovery mechanisms that enhance resiliency and enable us to rapidly recover and deliver amazing results.

Software will be at the heart of turning science fiction into reality in the space domain.