31st Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 13-14, 2015

# THE NEED FOR MODULAR CYBERSECURITY IN SPACE SYSTEMS

**Srikant Mantravadi**
Technica Corporation, smantravadi@technicacorp.com

## ABSTRACT

As the space industry moves toward smaller, lighter and more connection-aware systems, the cybersecurity industry needs to modify some of its approaches to provide the requisite cyberdefense capability needed to protect these systems in a congested and contested environment. The author highlights innovative work in the field while offering cautionary notes on relying too much on today's commercial solutions. The author also has a recommended roadmap for space systems to achieve cybersecurity objectives.

## EXECUTIVE SUMMARY

All systems including space systems have to ensure data integrity, protection, and confidentiality. The criticality of information needs to be the driver. Space systems provide critical command, control and information to warfighting and commercial customers. The data hosted on these systems are targets of thieves, provocateurs, and other ill-minded. When we focus on the data, the approaches to cybersecurity become more specialized and implementable.

In the current space landscape, with the desire for smaller more agile systems make cybersecurity a more ubiquitous challenge. A fundamental principle of cybersecurity systems involves the idea that a larger number of connected systems require more security and increase the "attack surface." More systems also mean a greater risk of compromise and a greater risk of data loss. The National Institute of Standards built a cybersecurity framework that focuses on the Continuous Diagnostics and Monitoring capability. CDM asserts that good systems engineering processes, coupled with standardized tools provide a predictable and repeatable cybersecurity strategy. Using the NIST framework for space systems will require a paradigm shift from the current "implement cybersecurity" approach to the new focus on continuous diagnostics.

However, space systems have been operating in a continuous diagnostics model since their inception. For example, monitoring status and health of the satellite is a required element of satellite operations. So ingesting continuous cybersecurity monitoring into space operations is more seamless than other systems. The NIST framework describes a cycle of continuous diagnostics and monitoring. The CDM strategy involves constantly monitoring and characterizing networks. By understanding the normal and likely conditions under which space networks performs, the cybersecurity systems can then diagnose anomalies.

The innovative solutions under this CDM construct specifically involve integration of a suite of tools. Not one tool or software has the capability to fully meet all the CDM requirements. Therefore, the best approach is to identify the toolset required to implement the required diagnostics capability, use software development principles to incorporating the toolset reporting into a dashboard. The dashboard provides the diagnostics to allow for the security staff to change the security posture while accurately reporting the risk profiles. The largest benefit of this CDM concept is in its ability to deliver a modular cybersecurity platform. This modular approach allows for increased or decreased security controls to be implemented quicker with predictable, measurable and accurately reported results.

Today, these tools for monitoring are provided by commercial products originally designed for more permanently connected systems. Therefore adding these commercial technologies to the connection-aware but not necessarily perpetually connected space systems have their pitfalls. These pitfalls include configuration management, less than predictable diagnostic regime, and a riskier security posture specifically when

cybersecurity is not being constantly monitored. The NIST framework allows for cybersecurity operational performance tradeoff.

Even with the risks of commercial cybersecurity solutions, the need for modular cybersecurity in space systems cannot be understated. Using the NIST, Continuous Diagnostics and Monitoring framework allows space system designers to "plug" cybersecurity into any system, receive required data to make security posture and risk decisions. Then the implemented CDM system can assure the data is protected, vulnerabilities are identified and mitigated, and risk profiles are accurately communicated. This modular CDM approach provides the best option to protect the current and future generation of space systems.

## INTRODUCTION

The problem of cybersecurity in persistently connected systems is amplified when focusing on space systems that may or may not be connected to cybersecurity capabilities. Documented instances of penetration and compromise of "closed" systems supporting satellite and ground systems further exacerbates the issues.

### *Background*

The best analogy I can use to describe the current state of the cybersecurity landscape is that of a casino. Anyone who has been to a casino recognizes that the odds are stacked in the favor of the "house." The analogy is similar in cybersecurity. In fact, the odds are so stacked against the designers and implementers of network systems, those odds cannot even be calculated. The "house" does not have any regulations to follow. There is unlimited budget and no limits. The stakes are higher than in any casino and the dealers don't even identify themselves.

Space system cyberspace security is even more challenging. Often the network is not perpetually connected; furthermore, the systems are very dependent on legacy technology, and rely on obscure and often large datasets. The ways these systems were built often are not very conducive to implement modern technologies as an overlay. Modernization in cybersecurity approaches cannot be as rapidly adopted to these space systems are they are on more connected systems.

### *Definitions*

The best place to begin is to accurately define terms. Here is a table of definitions that will be used throughout this document

| **Concept** | **Definition** |
|---|---|
| Cyberspace Security | The processes and tools used to secure information on a network |
| Connected Network | Networks that rely on data and information from other networks to accomplish their primary purpose. Example: Air Force Satellite Control Network |
| Modular | The development of a set of tools that can be upgraded, removed and replaced as required to meet technical requirements |

Figure 1: Definitions

### *Problem Statement*

The current threat landscape looks like the following:

**What is the Problem?**

- Every Three Days (on Federal networks):
  - Trillions of cyber events
  - Billions of potentially defective hardware, software, and account changes
  - Millions of attempted attacks at Internet speed
  - Thousands of new flaws introduced
  - Hundreds of successful attacks

- Every Three Months:
  - Over 10,000 successful attacks
  - An unknown number of these attacks are repaired
  - Terabytes of data are stolen
  - Over 7,200 reports are written, labor hours wasted when the reports are not used
  - Even when these reports are used, they only provides only a snapshot in time vs. real-time identification and mitigation of problems

This paper attempts to chart the landscape for architecting and implementing modular cybersecurity approaches, while providing for cautionary notes on the commercial practices occurring today where some

companies will promise an approach from a persistently connected environment will seamless transfer to space and other connection-aware but not necessarily connection-dependent systems.

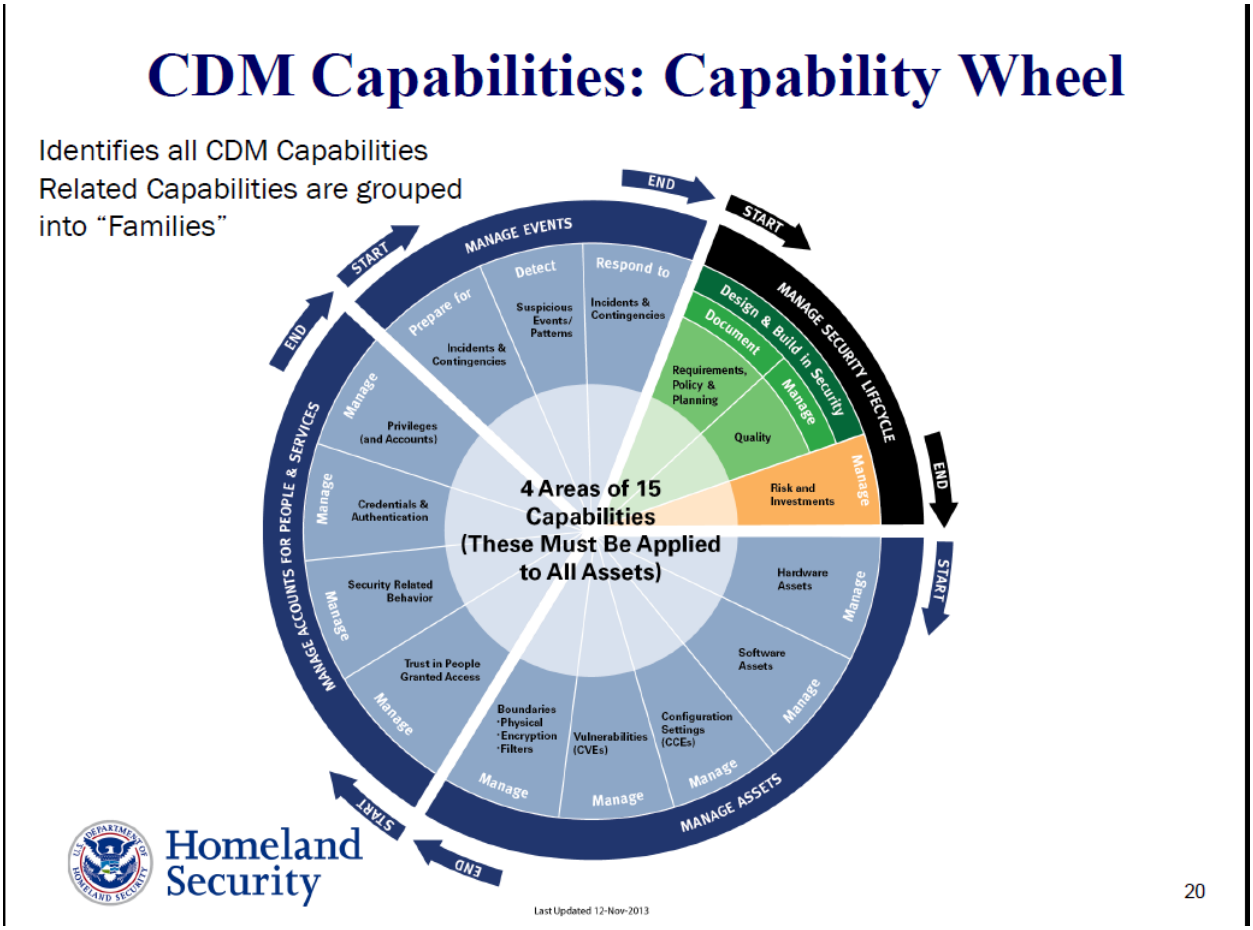
## MODULAR CYBERSECURITY

***Continuous Diagnostics and Mitigation***

According a recent CSIS report., 75% of the attacks use known vulnerabilities that could be patched; more than 90% of successful attacks require only the most basic techniques; and 96% of successful breaches can be avoided if the victim puts in place simple or intermediate controls. It also found that Continuous Diagnostics and Mitigation stops 85% of cyber-attacks by searching for, finding, fixing, and reporting the worst cyber problems first in near-real time. It also enables system administrators to:

- Respond to exploits at network speed
- Fulfill A-130 responsibilities as intended
- Implement NIST Publications on Continuous Monitoring (800-137 and parts of 800-37)
- Use strategic sourcing to lower costs[1]

The Department of Homeland Security established a program to provide four fundamental capabilities to provide network continuous diagnostics and mitigation. The figure below outlines the capabilities.




[1] NIST Special Publication 800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. p. 48. http://dx.doi.org/10.6028/NIST.SP.800-53r4 National Institute of Standards.

Figure 2 – CDM Capability Wheel[2]

These four areas refer to all assets on these networks. However, the monitoring and diagnosing of the networks do not have to be conducted perpetually.

Another significant requirement of CDM is the need for modularity The below slide reflects the key principles of modularity.

# Modular Capabilities

- Each CDM capability should (to the extent possible):
  - Address a distinct attack type (have a distinct purpose)
  - Collectively, the CDM capabilities should protect from all relevant attack types.
- CDM capabilities interact and support each other. For example:
  - Knowing what devices you have allows you to know where to look for software.
  - Knowing what software you have allows you to know what settings you need to check.
- Being able to implement capabilities individually, or a few at a time, simplifies implementation.
  - The capabilities are designed to allow be implemented incrementally.
  - The performance metrics are designed to show incremental progress within each capability.
- **So, you can eat the elephant one bite at a time.**

Figure 3: Modular Capabilities[3]

Identification of capability implementation individually and incrementally is a profound change for the cybersecurity community. The paradigm shift from an all or none approach to a modular approach allows for a broad acquisition strategy but also a measured delivery as to not impair operational activities

[2] CDM Training Presentation, Slide 20. www.dhs.gov
[3] CDM Training Presentation, Slide 45. www.dhs.gov.


Figure 4: CDM Implementation Approach[4]

DHS's intent is a 72-hour scanning cycle but that is based on a connected system with multiple users. The implementation from a space systems perspective can be focused on the threats and the specific nature of the network. If a system has a broad community of users who can initiate data gathering, that system could move closer to a 72 hour cycle, while a smaller user community and less data generation from users may be scanned at a more measured rate. In other words, the more the scanning, the more assurance of security but also the greater the need for network-connectedness.

***Enabling Capabilities***

In order to accurately and effectively implement CDM, three major enabling capabilities are required:

- Dashboards

[4] CDM DHS Training, Slide 46

- Scoring and Grading
- Maturity Metrics

The dashboard capability provides a snapshot to operational users, decision-aiding information to adequately identify the worst risks first, the status and health of their network and "what-if" scenarios. RSA Archer's dashboard is discussed in the innovative approach section of this paper. The need for a scoring and grading scheme cannot be overemphasized. The scoring factor is simply calculated. The base score is an assessment on how much a specific vulnerability if exploited affects the overall security of the network.

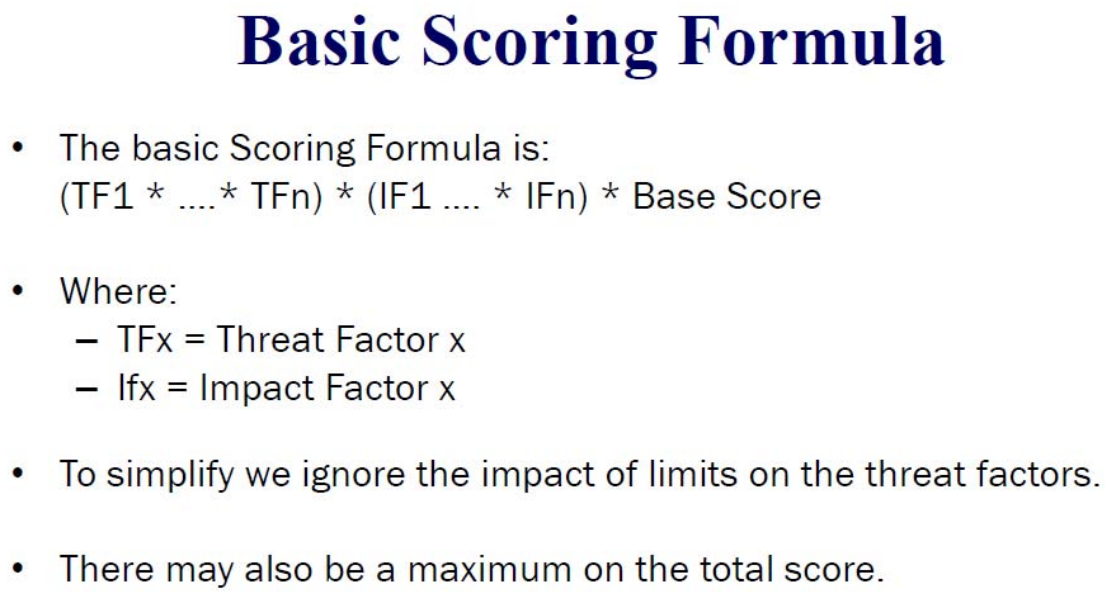



Figure 5: CDM Scoring Formula[5]

[5] DHS CDM Training, Slide 85. www.dhs.gov

Finally, a maturity model was developed to account for overall implementation and the overall status of the network's Continuous Diagnostics and Mitigation capability. The figure below illustrates the model's power.

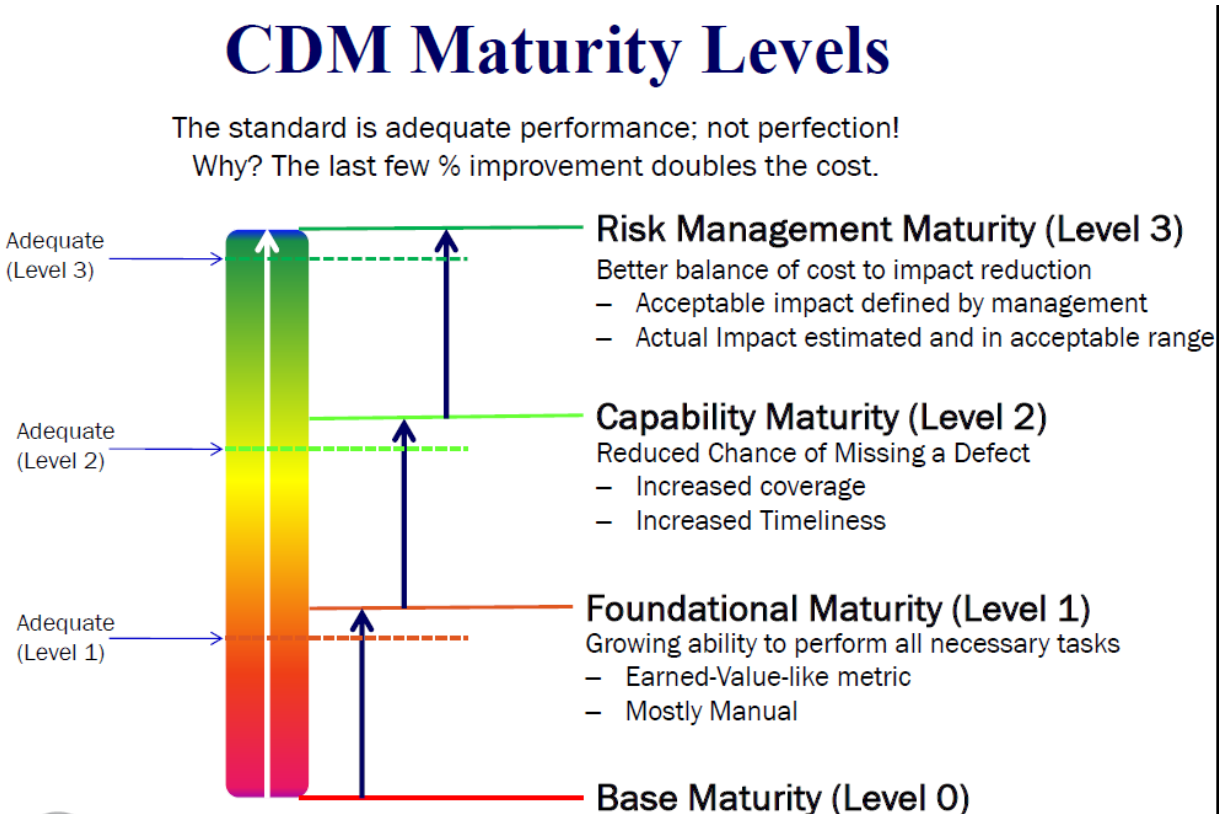



Figure 6: DHS CDM Maturity Levels[6]

Greater maturity can be achieved, measured, changed, and remeasured using these enabling capabilities. Especially attractive to space systems has to be the modular approach as well as how the CDM strategy allows for system owners to achieve the Risk Management Framework (RMF) security accreditation process the Department of Defense is currently implementing. The below figure illustrates this "realization "effectively.

[6] DHS CDM Training. Slide 99. www.dhs.gov.

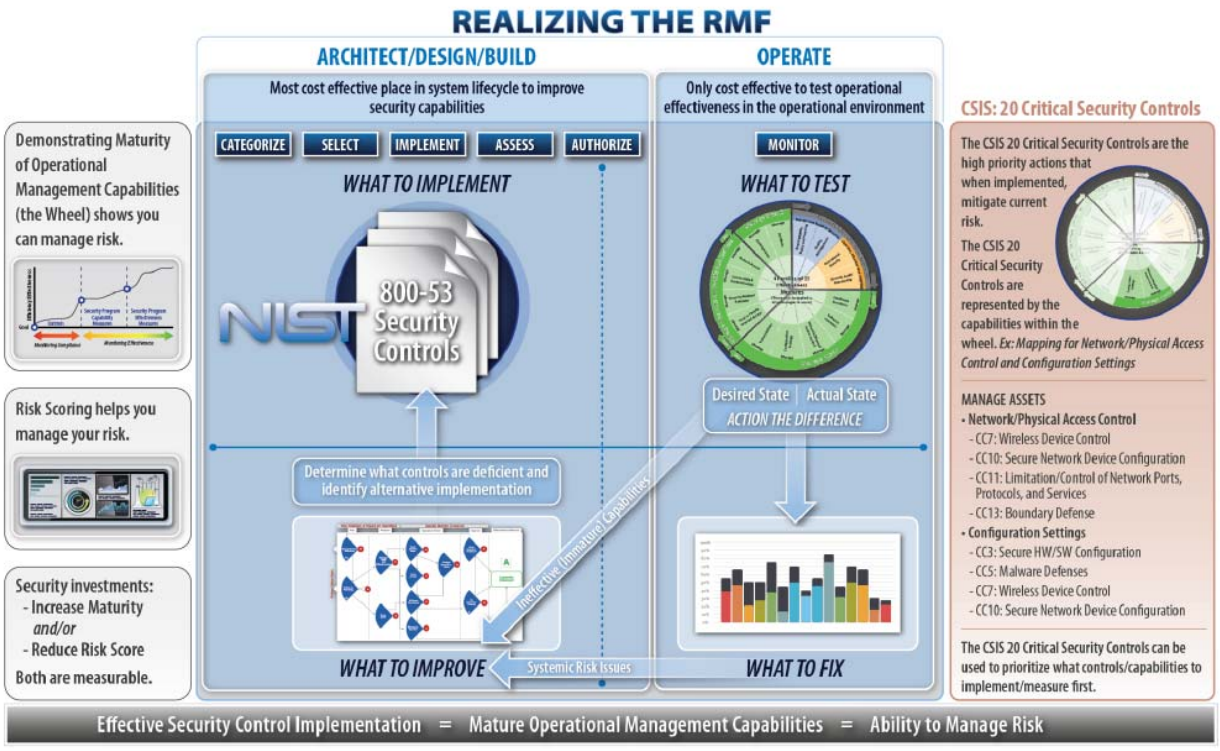



Figure 7: Realizing the Risk Management Framework[7]

## INNOVATIVE SOLUTIONS

Within the overall cybersecurity space, it is very important to identify innovation is very rapid. Innovation is observable in two specific areas. Obviously commercial industry has been focused on tools that support the required capabilities for core monitoring and diagnostics capabilities.

For the core capabilities, finding multiple capabilities "out-of-the box," is the most promising. The below table identifies good capabilities to provide solutions to CDM capability requirements.

| Capability Requirement | Definition | Innovation |
|---|---|---|
| **Boundary Control** | | |
| Physical Boundary Control | Preventing data loss from the physical boundary | Base-Layer |
| Virtual Boundary Control | Preventing data loss from the virtual boundaries | Fireye |
| Network Boundary Control | Preventing data loss from the network boundaries | Symantec Data Loss Prevention |
| **Identity and Access Management** | | |
| Privilege Management | Managing individual authenticated users network and data management privilege | Technica's Secure Token Service |
| Trust Management | Managing individual authenticated | Technica's FUNL coupled with |

[7] DHS CDM Strategic Plan, p. 15. www.dhs.gov

| | | |
|---|---|---|
| | user activity on the domain | individually developed analytics engines |
| Access Management | Managing individual user access | Technica's Secure Token Service |
| Asset Management | | |
| Hardware Asset Management | Identification and management of hardware assets | Symantec End Point Manager |
| Software Asset Management | Identification and management of software assets | Symantec End Point Manager |
| Configuration Setting and Control | Ensuring compliance with network standards for hardware systems | Forescout |

Figure 8: Innovation in CDM on Core Capabilities

Core capabilities are fundamental of course, but innovation continues in the areas of enabling capabilities as well. The below table identifies some of these innovative approaches:

| **Capability Requirement** | **Definition** | **Innovation** |
|---|---|---|
| **Meta-Capabilities** | | |
| Requirements Management | Analyzing the implementation of capabilities against baseline requirements | RSA-Archer Dashboard |
| Prepare for Action | Identification of the resources required to take action against threats | RSA-Archer Dashboard |
| Respond for Action | Response action tracking and after-action assessment | RSA-Archer Dashboard |
| **Implementation** | | |
| CDM as a Service | Deliver cybersecurity as a service | Technica's Cybersecurity Special Purpose Processing Node |
| **Enabling Capability** | | |
| Big Data Characterization | Rearranging data using graph analytics to identify duplication of data and deliver smaller data set to data analytical engines | Technica's FUNL |

Figure 9: Innovation in CDM Non-core Capabilities

***Use Cases:***

*RSA – Archer*

The RSA-Archer Security Operations Dashboard capability is specifically designed to provide the overall framework for managing CDM solutions. The need for a dashboard that provides "at-a-glance," common picture of the state of a network, deliver "what-if" scenario analysis, and deliver recommendations to the operational users. RSA-Archer brings the better of two worlds, the software views were designed for cybersecurity operations so the right types of "default" views are available but specific customizations are easily executed.

*CDM as a Service*

As in most programs or new capability areas, implementation in an enterprise can be time consuming, Since, the values of modularity necessitates agile and flexible design and delivery. Technica has developed a capability

offering around the core capabilities of the CDM program called a CDM Special Purpose Processing Node or C-SPPN. The SPPN will leverage key partners such as Symantec, RSA, Fireye and other innovative companies to offer a Software as a Service+ offering. Most of the networking components required by CDM are software-based tools. However, just providing software is not sufficient to meet the requirements of space systems. The understanding of DoD requirements as well as implementation details of systems are critical to the delivery of a holistic CDM solution. What if you could "hire" a capability to scan, report, recommend and fix your most critical vulnerabilities. By "bundling requirements," into common offerings, the C-SPPN will be able to offer customers on-demand cybersecurity in accordance with NIST requirements.

*FUNL (Big-Data)*

Large enterprise systems will produce large amounts of complex datasets. Efficient CDM implementation will need ways to characterize, deduplicate and "funnel" the smaller dataset into analytic capability. Technica used graph-analytics to further refine large datasets and execute the characterization and deduplication functions. The FUNL effort will allow all system owners to perform data analytics specifically cybersecurity data analytics required to meet the diagnostic and mitigation requirements.

## CAUTIONARY NOTES

***Risk***

The current thinking about risk and its underlying implementation in cybersecurity prescribes a "good-enough" idea. Defining what is "good enough" is domain and system specific. 72 hours on 80% of network assets may not be sufficient for critical mission applications. Implementing shorter scan times and/or securing larger numbers of assets will cost more but may be required to meet risk profiles.

***Overreliance on Commercial Technology***

Commercial industry has built their tools on a "good enough" approach as well. The large virus signature manufacturers will take care of exploited vulnerabilities that are used by a large set of their customers. However with space systems and other unique systems, there will be a need for vulnerability management capabilities not easily "fixed" with signatures, they will require software development efforts. A cadre of cyberdefense professionals who focus on the remaining 20% whether it is for scale or technical complexity, are required to close those vulnerabilities that affect space systems.

***What about SCADA?***

The risk of physical and control system compromise has been well-documented. The current implementation of CDM is more focused at the IP layer and needs to be cognizant of other layers. The CDM framework can and does support physical, management and legacy data networks. The space of SCADA attack detection and mitigation has been advancing in capability and capacity. Investment in niche capabilities for SCADA networks will be required as well.

***Data Analytics***

A critical component of CDM involves behavior management. In order to perform behavior management, data analytics design and execution is critical. Data is analyzed to determine anomalous and predictive behavior. The lack of data analytics capability for space systems, data strategies for legacy space systems present a challenge to provide behavior management.

## CONCLUSION

### *Takeaways*

The need for modularity in cyberspace security for space systems is indisputable. The paper presents the following takeaways:

1. Technology pace of change is exponentially difficult to keep up with
2. Systems of Systems Engineering is critical
3. Modularity is necessary
4. Modularity is possible
5. Risk Management definitions are paramount
6. Dashboards and constant measurement are critical enabling capabilities
7. Commercial Technologies are exciting but pose risks
8. Implementation strategy will be critical