National Defense Industrial Association
October 2019

# Intelligence Implementation of Acquisition Agility and Integration with Systems Engineering Processes

**Mr. Dwayne Hynes**
**Acquisition Intelligence Division, ASD(A)/OUSD(I)**

**Mr. John Daly**
**Booz Allen Hamilton**

***October 2019***

***Effective integration of intelligence can save time, money and ensure programs can defeat future threats***

# INTEL: What it is; What it isn't

- This covers:
  - ✓ What is Acquisition Intelligence (Acq Intel)
  - ✓ Three major Touchpoints for Acq Intel
  - ✓ Managing Requirements and Specifications
  - ✓ Acquisition Agility Act (NDAA 2017) and Threat provisions
  - ✓ Intelligence Acquisition Agility Working Group
  - ✓ Some Examples

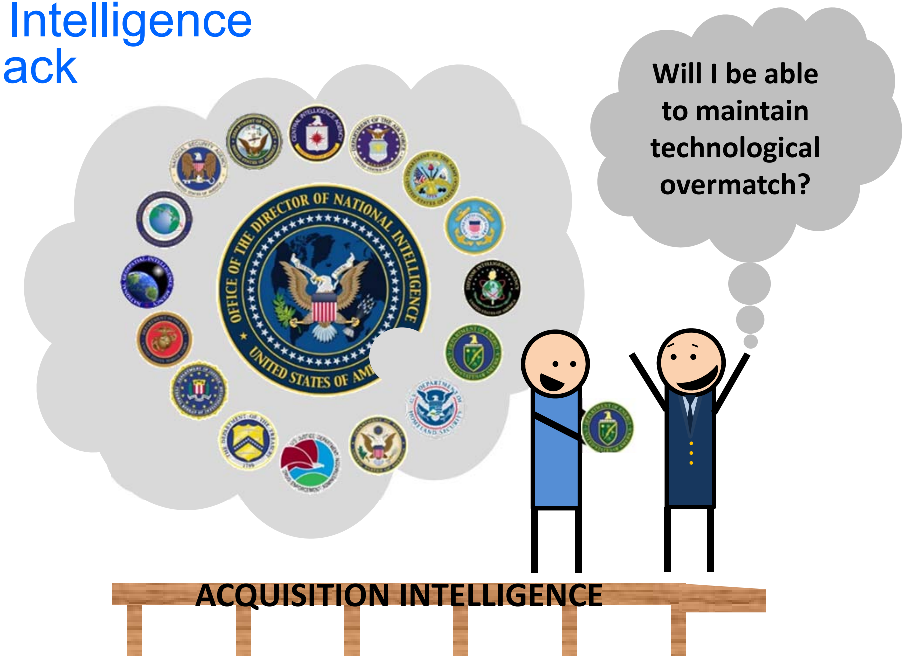
***Enabling Decisive Operations While Transforming in the Breach***

# What Is Acquisition Intelligence?

**Intelligence** = Data + Analysis

**Acq Intel** = Intel + Requirements/Acquisition Knowledge
+ Application/Integration of Intelligence
+ Data driven feedback

**In Layman's Terms:** *Acq Intel is the application of intel expertise to inform trade-space decisions; translate requirements into engineering specifications; and provide awareness of intel risks in a program's cost, schedule & performance.*



# Benefits of Acq Intel

## *More than the traditional threat assessment!*

Threat Assessments only part of Acq Intel—application key

## *Realistic Cost Estimates*

Early identification of intel infrastructure needs

Earlier deficiencies resolution

Intel support integrated into life cycle cost

## *Schedule*

Identify and resolve schedule conflicts involving intel data availability

## *Performance*

Realistic requirements and translation into specs

Build intel support structure to maximize system performance

Field integrated capability with first increment

# Trivia

**Question: How many acquisition intelligence professionals are there in the Services?**

**Answer: Currently, there are 470 Acquisition Intelligence Professionals (0.34% of the combined MILDEPT acquisition workforce)**

**Army = 99**
**Navy = 84**
**Marine Corps = 9**
**Air Force = 278**

# Three Major Touchpoints

## REQUIREMENTS

CBA – AoA – ICD/**Draft CDD**

MS A

Goal: Requirements informed by intelligence

Participate in JCIDS

KPPs/KSAs threat informed

**Define trade space (T/O)**

Scenario review

Verify planning figures

Reliance on threat data

Provide the “So what”

Products:

- VOLT and CIPs
- Threat paragraph in ICD/CDD and TEMP
- Initial IMD requirements
- Threat Rep Rqmts

## ACQUISITION

CDD - **Development RFP** - Design Reviews

MS B

- Goal: **Effective Engineering solutions**
- Participate in RFP
- Refine trade space
- Identify key technology
- Technology protection
- Reliance on threat data
- Operational environment
- Provide the “So what”

Products:

- VOLT Refresh
- CIP Status Update
- IMD Sufficiency
- Threat Rep Status for T&E

## TESTING & EVALUATION

TEMP - SEP w/DSM - CPD

**Operational Testing**

MS C

- Goal: **Threat representations available to support testing**
- Availability of threat data
- Validation and accreditation
- OPFOR training
- On site threat validation

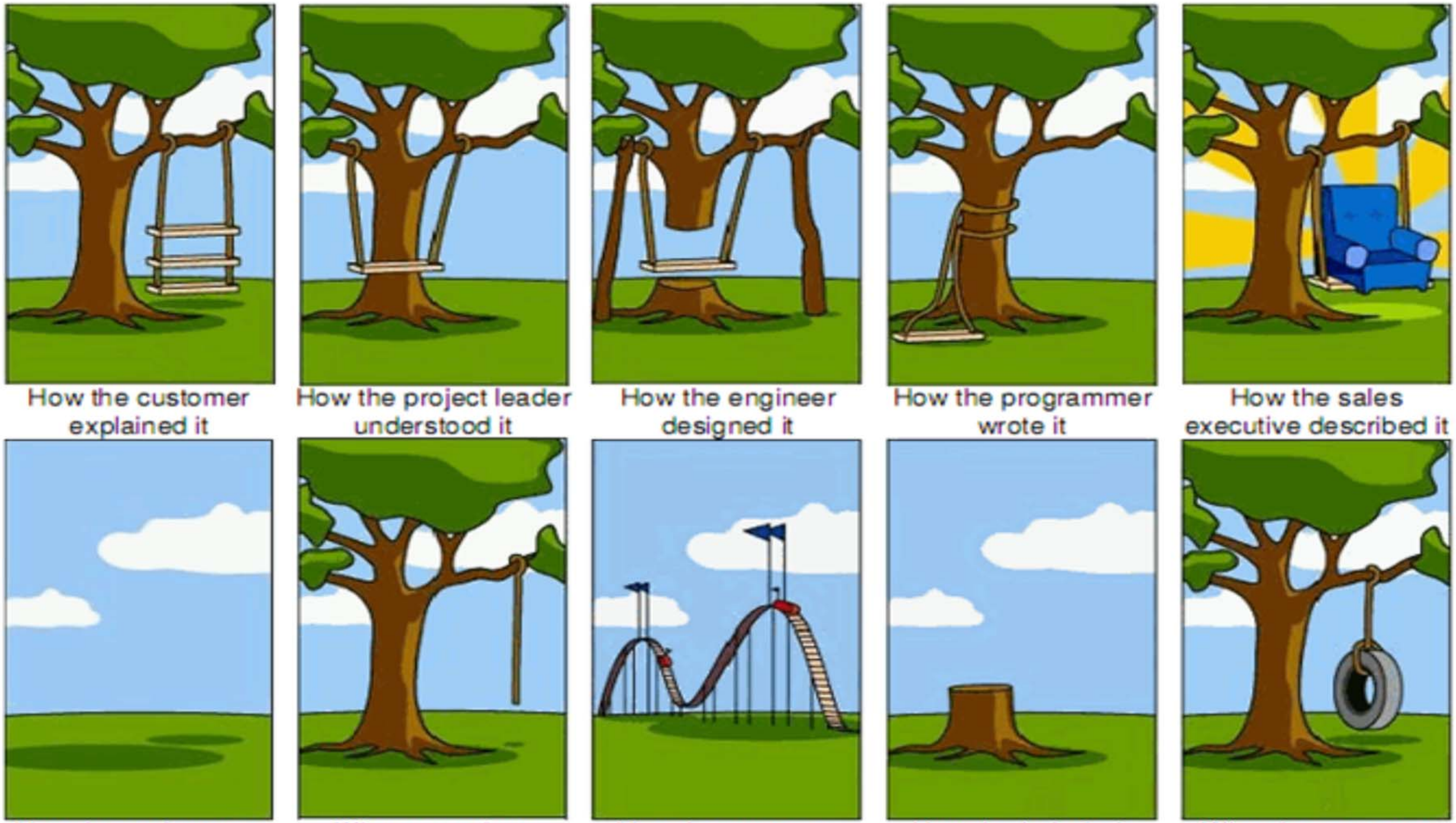
Products:

- VOLT Refresh
- CIP Status Update
- IMD to support T&E
- VV&A of Threat Reps for T&E
- Update to Lifecycle Sustainment Plan

***If we get nothing else right…just sitting down during these three events***

# Managing Requirements

- In the course of developing performance specifications and/or interface control documents, 1000s of requirements (SHALL statements) can be generated.
- Each of those requirements has to be justified because each “SHALL statement” costs money.
- **Traceability** is how that justification is accomplished
- To help manage each of those requirements, some programs rely on commercial **Model-Based Systems Engineering Tools** (e.g. (MagicDraw, Rational Rhapsody, Visual Paradigm…., etc.) and specific requirements management tools: ( e.g Rational DOORS, Enterprise Architect, Jira etc.).
  - These Digital Engineering tools allow connection of requirements between specifications (traceability) and enforce configuration management and history.
  - The MBSE tools allow direct modeling of system performance
  - **Acquisition intelligence can play a vital role in tracking threat against system performance specifications and provide early warning**



How the customer explained it

How the project leader understood it

How the engineer designed it

How the programmer wrote it

How the sales executive described it

How the project was documented

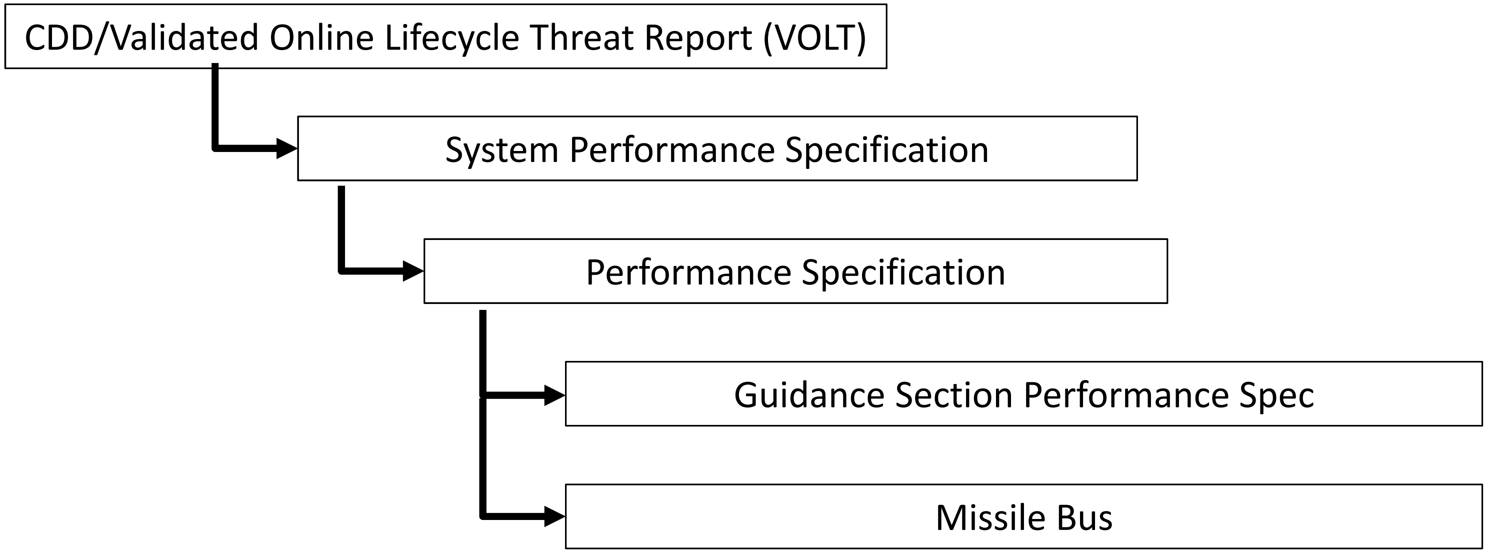
What operations installed

How the customer was billed

How the helpdesk supported it

What the customer really needed

# Traceability = Accountability



CDD/Validated Online Lifecycle Threat Report (VOLT)

System Performance Specification

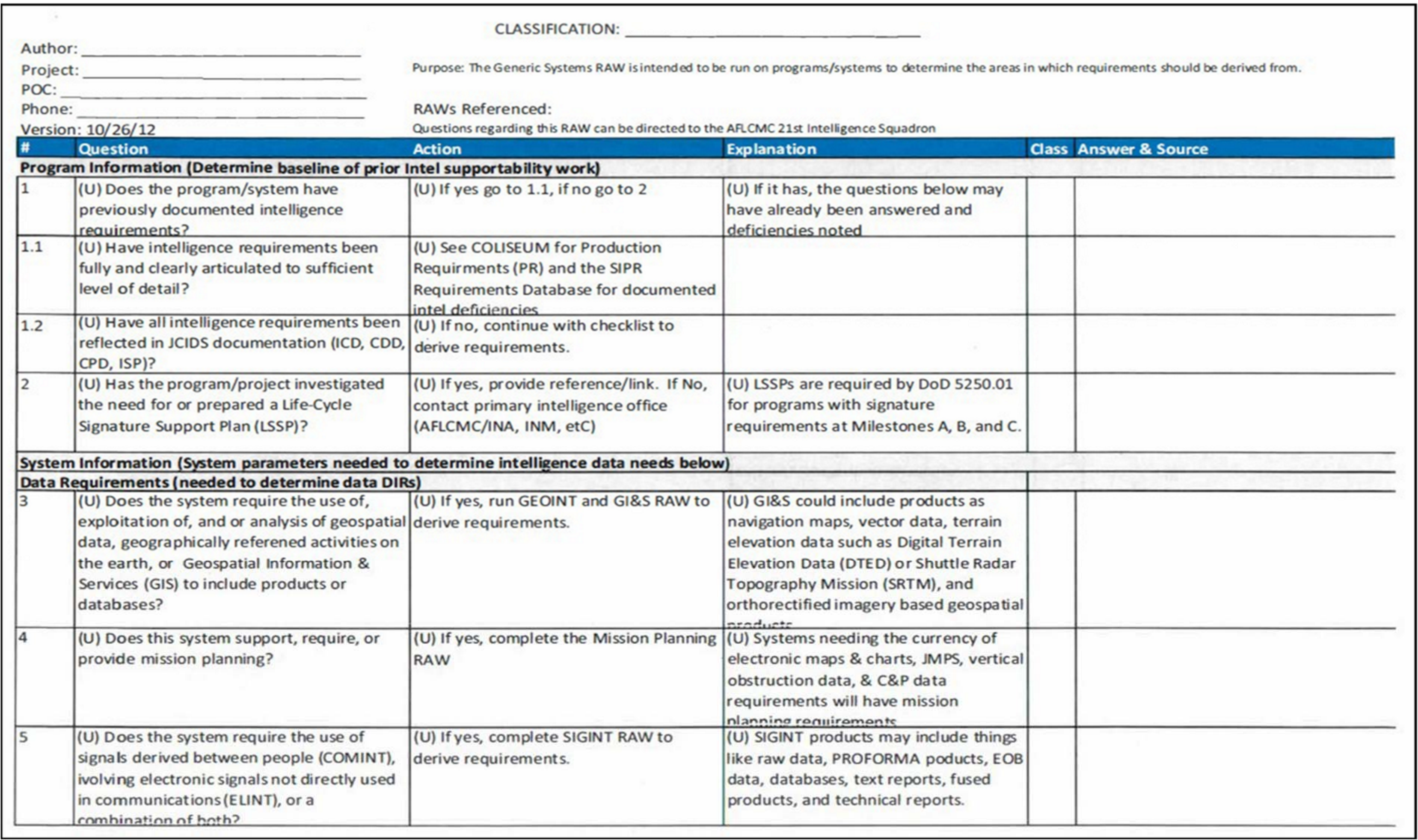
Performance Specification

Guidance Section Performance Spec

Missile Bus

**Requirements cost money and best intentions are still GOLD PLATING.**

# Traceability = Accountability
# Intelligence Data Dependencies



CLASSIFICATION: ______________________________

Author: ______________________________

Project: ______________________________

POC: ______________________________

Phone: ______________________________

Version: 10/26/12

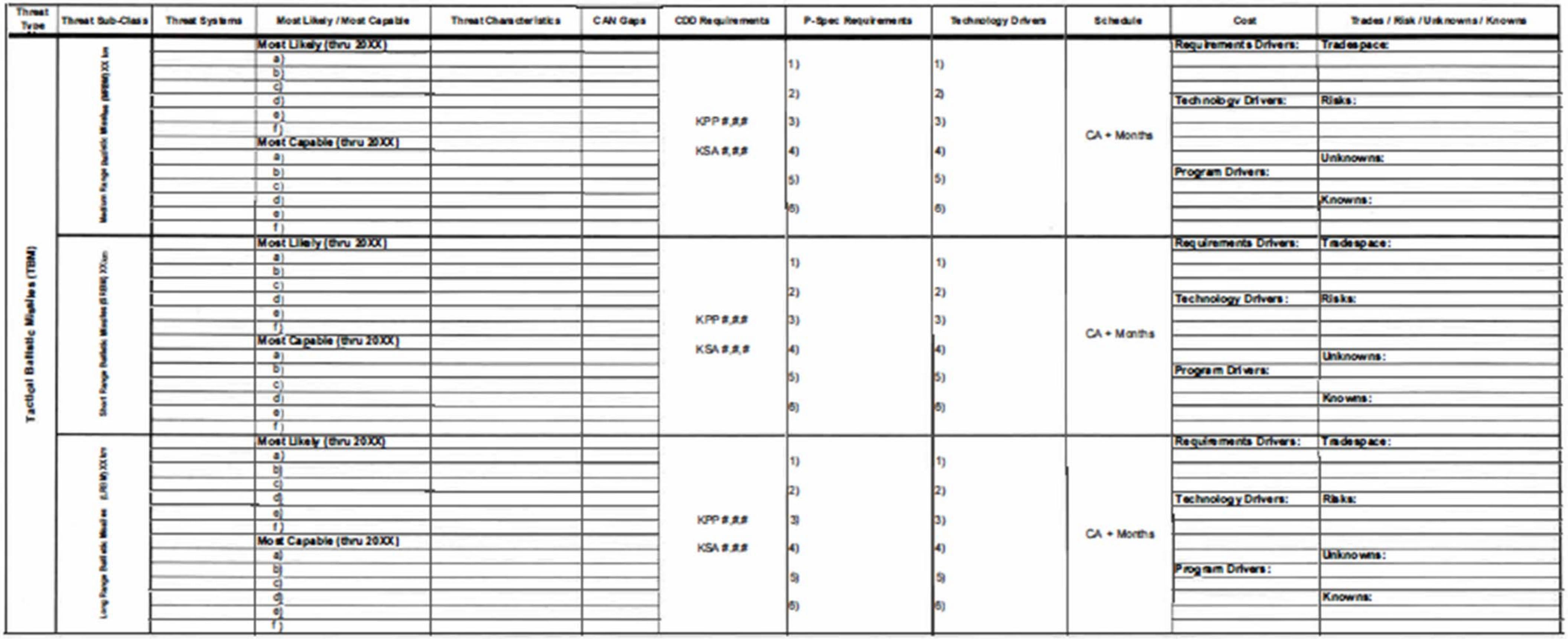
Purpose: The Generic Systems RAW is intended to be run on programs/systems to determine the areas in which requirements should be derived from.

RAWs Referenced:

Questions regarding this RAW can be directed to the AFLCMC 21st Intelligence Squadron

| # | Question | Action | Explanation | Class | Answer & Source |
|---|---|---|---|---|---|
| **Program Information (Determine baseline of prior Intel supportability work)** | | | | | |
| 1 | (U) Does the program/system have previously documented intelligence requirements? | (U) If yes go to 1.1, if no go to 2 | (U) If it has, the questions below may have already been answered and deficiencies noted | | |
| 1.1 | (U) Have intelligence requirements been fully and clearly articulated to sufficient level of detail? | (U) See COLISEUM for Production Requirments (PR) and the SIPR Requirements Database for documented intel deficiencies | | | |
| 1.2 | (U) Have all intelligence requirements been reflected in JCIDS documentation (ICD, CDD, CPD, ISP)? | (U) If no, continue with checklist to derive requirements. | | | |
| 2 | (U) Has the program/project investigated the need for or prepared a Life-Cycle Signature Support Plan (LSSP)? | (U) If yes, provide reference/link. If No, contact primary intelligence office (AFLCMC/INA, INM, etC) | (U) LSSPs are required by DoD 5250.01 for programs with signature requirements at Milestones A, B, and C. | | |
| **System Information (System parameters needed to determine intelligence data needs below)** | | | | | |
| **Data Requirements (needed to determine data DIRs)** | | | | | |
| 3 | (U) Does the system require the use of, exploitation of, and or analysis of geospatial data, geographically referened activities on the earth, or Geospatial Information & Services (GIS) to include products or databases? | (U) If yes, run GEOINT and GI&S RAW to derive requirements. | (U) GI&S could include products as navigation maps, vector data, terrain elevation data such as Digital Terrain Elevation Data (DTED) or Shuttle Radar Topography Mission (SRTM), and orthorectified imagery based geospatial products | | |
| 4 | (U) Does this system support, require, or provide mission planning? | (U) If yes, complete the Mission Planning RAW | (U) Systems needing the currency of electronic maps & charts, JMPS, vertical obstruction data, & C&P data requirements will have mission planning requirements | | |
| 5 | (U) Does the system require the use of signals derived between people (COMINT), ivolving electronic signals not directly used in communications (ELINT), or a combination of both? | (U) If yes, complete SIGINT RAW to derive requirements. | (U) SIGINT products may include things like raw data, PROFORMA products, EOB data, databases, text reports, fused products, and technical reports. | | |

# Traceability = Accountability
# Digitally Consumable



| Threat Type | Threat Sub-Class | Threat Systems | Most Likely / Most Capable | Threat Characteristics | CAN Gaps | CDD Requirements | P-Spec Requirements | Technology Drivers | Schedule | Cost | Trades / Risk / Unknowns / Knowns |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Tactical Ballistic Missiles (TBM) | Medium Range Ballistic Missiles (MRBM) XX km | | Most Likely (thru 20XX) | | | KPP #.#.#<br>KSA #.#.# | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | CA + Months | Requirements Drivers: | Tradespace: |
| | | | a) | | | | | | | | |
| | | | b) | | | | | | | | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | Technology Drivers: | Risks: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |
| | | | Most Capable (thru 20XX) | | | | | | | | |
| | | | a) | | | | | | | | Unknowns: |
| | | | b) | | | | | | | Program Drivers: | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | | Knowns: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |
| | Short Range Ballistic Missiles (SRBM) XXkm | | Most Likely (thru 20XX) | | | KPP #.#.#<br>KSA #.#.# | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | CA + Months | Requirements Drivers: | Tradespace: |
| | | | a) | | | | | | | | |
| | | | b) | | | | | | | | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | Technology Drivers: | Risks: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |
| | | | Most Capable (thru 20XX) | | | | | | | | |
| | | | a) | | | | | | | | Unknowns: |
| | | | b) | | | | | | | Program Drivers: | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | | Knowns: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |
| | Long Range Ballistic Missiles (LRBM) XX km | | Most Likely (thru 20XX) | | | KPP #.#.#<br>KSA #.#.# | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | 1)<br>2)<br>3)<br>4)<br>5)<br>6) | CA + Months | Requirements Drivers: | Tradespace: |
| | | | a) | | | | | | | | |
| | | | b) | | | | | | | | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | Technology Drivers: | Risks: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |
| | | | Most Capable (thru 20XX) | | | | | | | | |
| | | | a) | | | | | | | | Unknowns: |
| | | | b) | | | | | | | Program Drivers: | |
| | | | c) | | | | | | | | |
| | | | d) | | | | | | | | Knowns: |
| | | | e) | | | | | | | | |
| | | | f) | | | | | | | | |

# Why the Acquisition Agility Act?

Conventional Department of Defense (DoD) acquisition system (DAS) is "not sufficiently agile to support warfighter demands"

House Committee Report 114-102 accompanying the National Defense Authorization Act (NDAA) for Fiscal Year 2016 (FY16)

- *Does not respond rapidly enough to changes in technology and threat to respond with capability counters at the speed of relevance*
- *Is a linear model, an iterative model with continuous feedback required*

FY17 NDAA Acquisition Agility Act (AAA) changes the way capabilities are acquired so they are more flexible to:

- *React to and remain ahead of emerging threats*
- *Take advantage of emerging technologies*
- *Increase interoperability*
- *Reduce schedule/decrease cost*
- *Other sustainment benefits*

**AAA requires changes to the way we do acquisition and has far-reaching consequences to the Defense Acquisition System (DAS)**

# Key Threat Requirements in AAA (NDAA-17)

- (1)(a) MODULAR OPEN SYSTEM APPROACH REQUIREMENT: ”includes a subsystem or assembly that is likely to have additional capability requirements, is likely to change because of evolving technology or **threat**,”

MOSA Design Threat consideration

- (1)(b) PROGRAM CAPABILITY DOCUMENT: “a program capability document *(i.e. CDD)* for a major defense acquisition program shall identify and characterize — the extent to which requirements for system performance are likely to evolve during the life cycle of the system because of evolving technology, **threat**, or interoperability needs”

Requirements/JCIDS Threat consideration

- (2)(a) PROGRAM COST, FIELDING, AND PERFORMANCE GOALS: "incorporate program planning that anticipates the evolution of capabilities to meet **changing threats**, technology insertion, and interoperability”

Performance/Goals Threat consideration

**References:**

(1) SEC. 805. MODULAR OPEN SYSTEM APPROACH IN DEVELOPMENT OF MAJOR WEAPON SYSTEMS: ‘‘CHAPTER 144B—WEAPON SYSTEMS DEVELOPMENT AND RELATED MATTERS

(a) ‘‘§ 2446a. Requirement for modular open system approach in major defense acquisition programs; definitions”:

(b) ‘‘§ 2446b. Requirement to address modular open system approach in program capabilities development and acquisition weapon system design”

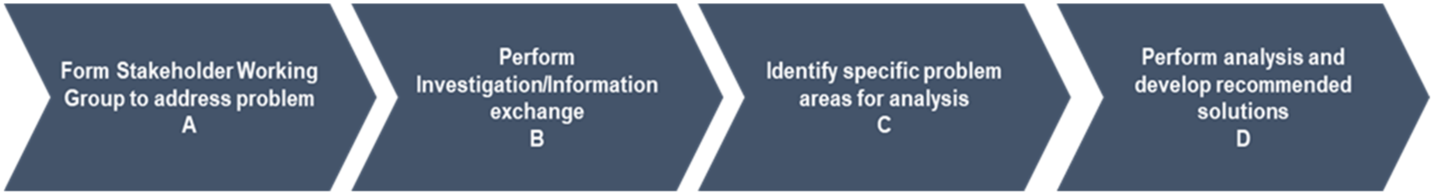
(2) SEC. 807. COST, SCHEDULE, AND PERFORMANCE OF MAJOR DEFENSE ACQUISITION PROGRAMS.: Chapter 144B SUBCHAPTER III—COST, SCHEDULE, AND PERFORMANCE OF MAJOR DEFENSE ACQUISITION PROGRAMS

(a) ‘‘§ 2448a. Program cost, fielding, and performance goals in planning major defense acquisition programs”

# The Intel-Acquisition Agility WG effort

## Areas of concentration over 6 months of meetings, analysis, and collaboration:

- **POLICY:** Better codifying and condensing Directive/Guidance/Standardizing policy for acquisition intelligence integration
- **INTELLIGENCE INTEGRATION WITH ACQUISITION** : Integrating intelligence processes for threat information in a construct applicable to acquisition systems engineering and program management
- **DIGITAL INTELLIGENCE** : *The opportunity to develop a Digital Intelligence paradigm to better support the acquisition community with integration of Intelligence into the Digital Engineering Ecosystem, including direct "machine-to machine" integration/automation*
- **CYBER CONSIDERATIONS:** Cyber was examined in multiple ways: as a component of threat to a DoD acquisition program's inherent capability, as a threat to the operation of DoD Intelligence- Acquisition processes, and as a DoD mission threat
- **INTELLIGENCE – SCIENCE AND TECHNOLOGY INTEGRATION:** Closer coordination between the Defense Intelligence and Security Enterprise (DISE) and S&T communities was explored, especially with a view towards the longer-range threat forecasting needs of the S&T community in evaluating and selecting technology options for implementation in the Department



Form Stakeholder Working Group to address problem
A

Perform Investigation/Information exchange
B

Identify specific problem areas for analysis
C

Perform analysis and develop recommended solutions
D

# Output from Intel-Acquisition Agility effort

- **Develop portfolio level, strategic sets of mission/capability-level integrated threat assessments**; tailored to support: acquisition outside of Major Defense Acquisition Programs that have dedicated VOLT support, capability requirements development, and S&T developmental planning efforts.
- **Enhance the Validated Online Lifecycle Threat (VOLT) process to be truly dynamic**; more frequently updated, and relevant across a wider range of programs and efforts with threat modules that can be readily tailored to support multiple program and efforts
- **Revise the Critical Intelligence Parameter (CIP) process**; expand CIPs at the strategic and portfolio level to monitor multiple programs and other non-traditional acquisitions (prototyping etc.) for vulnerabilities to threat and to alert decision-makers to systemic problems across swaths of capabilities in response to an emerging/changing threat.
- **Provide threat information – searchable, tailorable, and consumable**; *at the appropriate engineering level of specificity in a risk-based digital framework;*
- **Inform mission and developmental modeling and simulation with credible, attributed, and tailorable threat information and models**; *at a fidelity and resolution suitable to the analysis use.*
- **Develop a construct for intelligence support to O/S and reporting to support Agile Acquisition** in production and post production phases
- **Integrate intelligence considerations into contracting** to inform contracting organizations of the type of language and structure needed in a solicitation to obtain the desired result.
- **Supply Chain Threat monitoring**; investigate Supply Chain threat vulnerability in operational use with the appropriate organizations
- **Monitor cyber vulnerabilities** in the development and deployment of a Digital Intelligence capability;

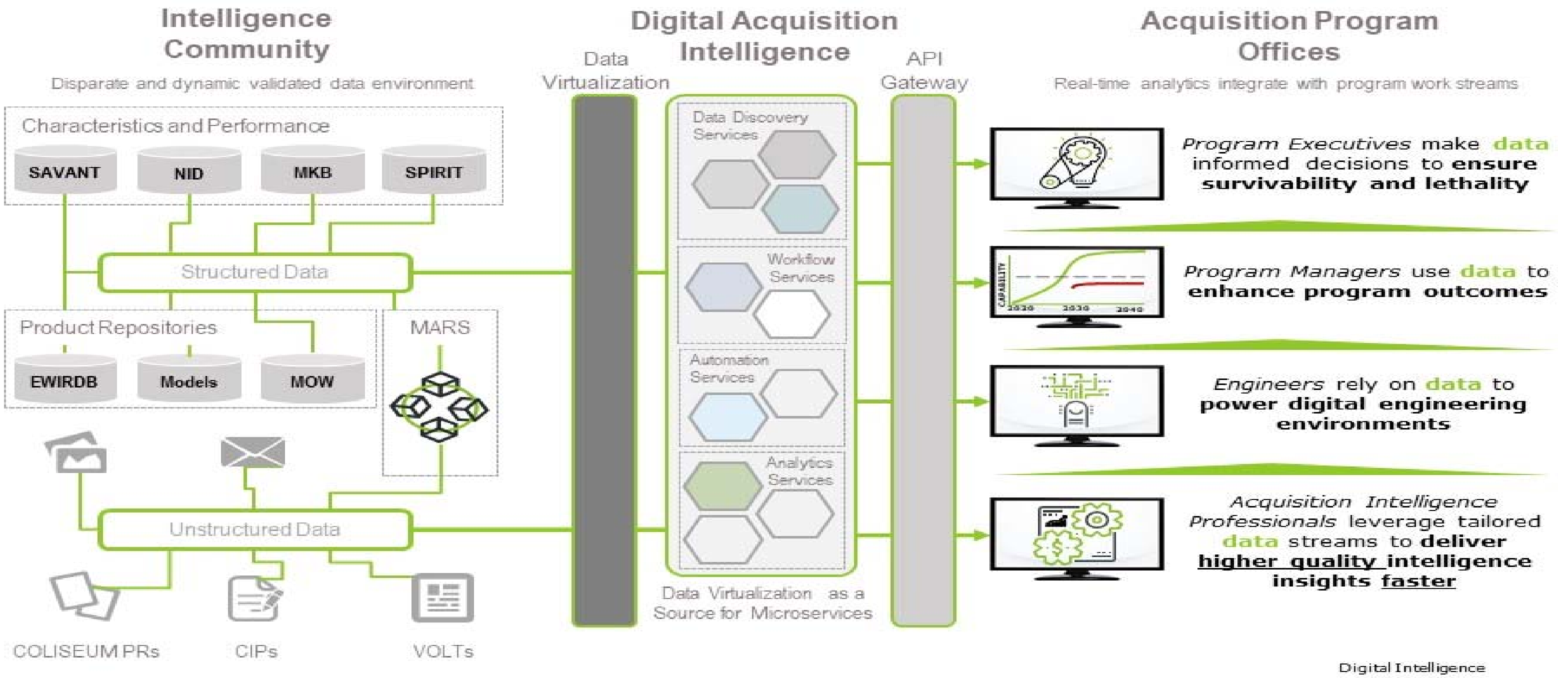
# More detail on key Output

**Provide threat information – searchable, tailorable, and consumable; at the appropriate engineering level of specificity in a risk-based digital framework;** this would link corresponding components, capabilities, sensitivities, and vulnerabilities of an acquisition program, or portfolio of programs to their Digital Engineering methodologies and tools. This Digital Intelligence concept would utilize a data-driven and comprehensive linkage across all aspects of an acquisition program or portfolio – identifying dependencies and interactions simultaneously.

- Continue development of a Digital Intelligence concept as a complement to, and use case of, Digital Engineering tools, frameworks, and methodology; inform an acquisition program's systems engineering, and program management/decision making with a current, comprehensive, and accessible view of relevant threat
- Transform intelligence support from a paper-based product to a parametric, digital construct
- Leverage the ISO/IEEE/DoD Systems Engineering Standard 15288. The Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on Contracts for Department of Defense Acquisition Programs and develop a recommended system engineering process standard for integrating Digital Intelligence into Digital Engineering

# Digital Intelligence

*Modernizing Intelligence Support to Improve Acquisition Outcomes*



## Intelligence Community

Disparate and dynamic validated data environment

## Digital Acquisition Intelligence

Data Virtualization as a Source for Microservices

## Acquisition Program Offices

Real-time analytics integrate with program work streams

*Program Executives* make **data** informed decisions to **ensure survivability and lethality**

*Program Managers* use **data** to **enhance program outcomes**

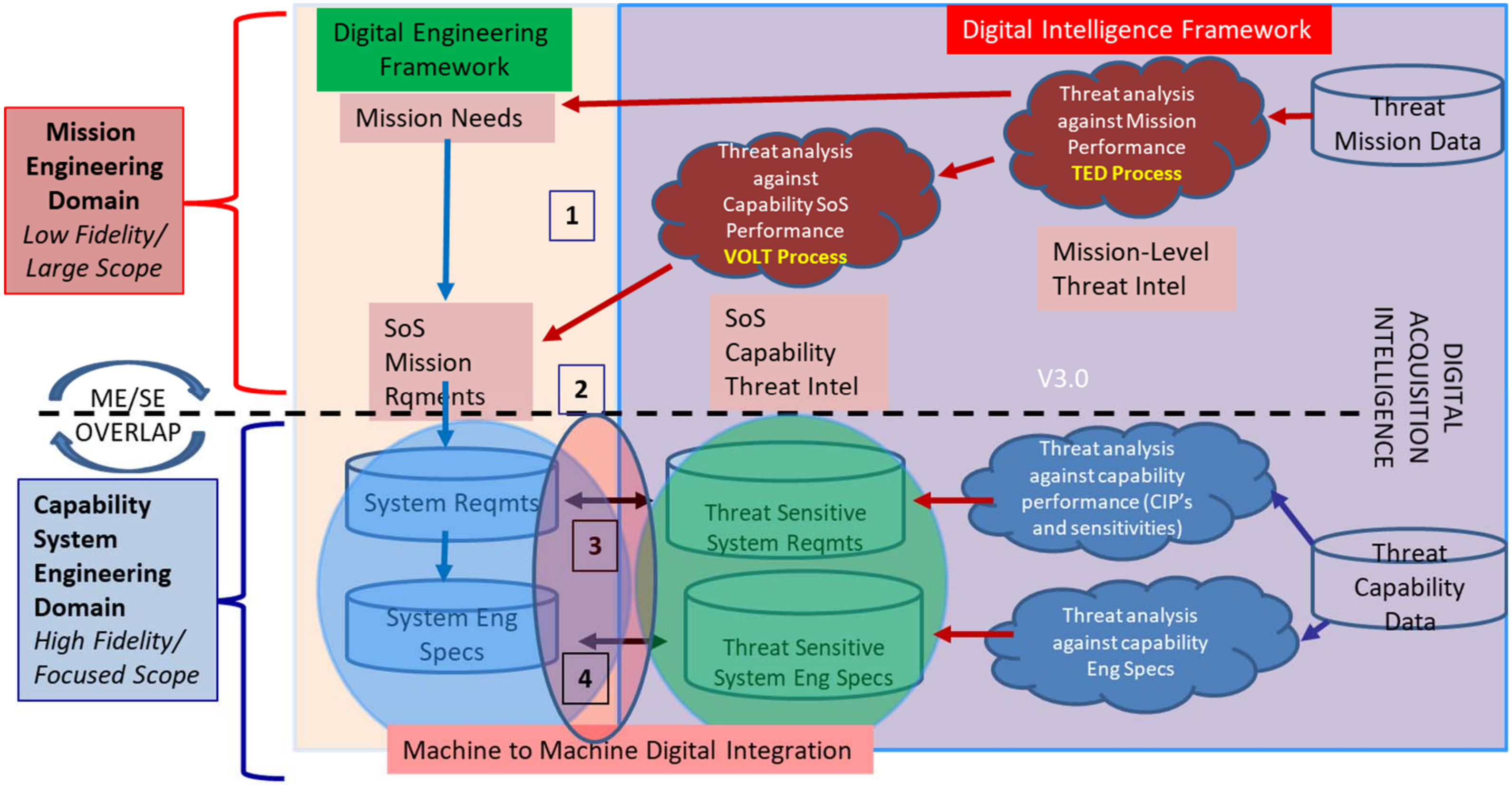
*Engineers* rely on **data** to **power digital engineering environments**

*Acquisition Intelligence Professionals* leverage tailored **data** streams to **deliver higher quality intelligence insights faster**

Digital Intelligence

***Contact:*** *AID | Dwayne Hynes, Deputy Division Chief – dwayne.d.hynes.civ@mail.mil | Maggie Jenkins, Deloitte Consulting– maggie.j.jenkins.ctr@mail.mil*

# DIGITAL INTELLIGENCE  Process


Mission Engineering Domain
*Low Fidelity/ Large Scope*
ME/SE OVERLAP
Capability System Engineering Domain
*High Fidelity/ Focused Scope*
Digital Engineering Framework
Mission Needs
1
SoS Mission Rqments
2
System Reqmts
3
System Eng Specs
4
Machine to Machine Digital Integration
Digital Intelligence Framework
Threat analysis against Mission Performance
TED Process
Threat Mission Data
Threat analysis against Capability SoS Performance
VOLT Process
Mission-Level Threat Intel
SoS Capability Threat Intel
V3.0
DIGITAL ACQUISITION INTELLIGENCE
Threat Sensitive System Reqmts
Threat Sensitive System Eng Specs
Threat analysis against capability performance (CIP's and sensitivities)
Threat analysis against capability Eng Specs
Threat Capability Data

# Future Cannon and Tradespace

And a story on why informing requirements with intelligence is so critical

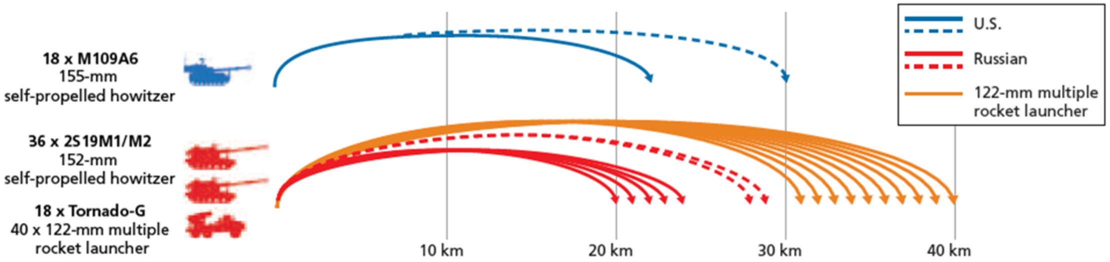
# From Requirements to Solutions

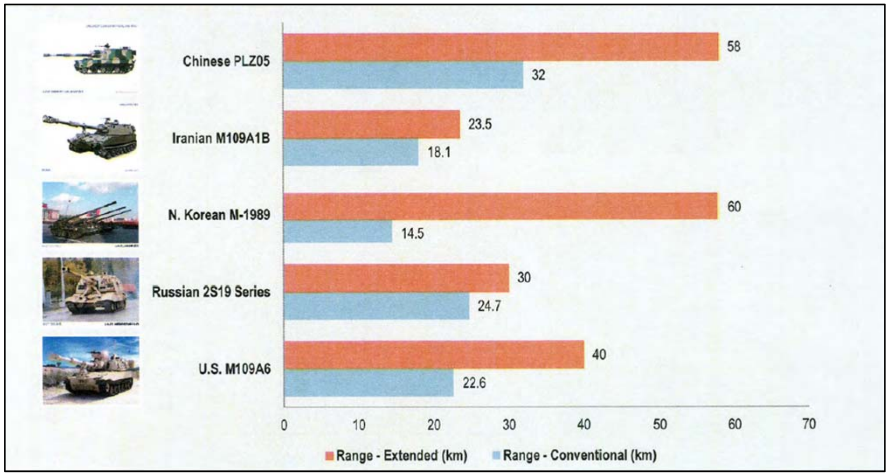
# Cannon Requirements Decision Space

| Parameter | Requirement | Impact | | | Threat |
|---|---|---|---|---|---|
| | | Cost | Schedule | Performance | |
| Weapon System Reliability | 75-83%? probability of completing an 18 hr combat mission; 62 hrs MTBSA | Increased test cost—test, fix | Increased testing time | Linked to operational need | High reliability—simple designs |
| Mobility | Similar as previous models | Development of improved engine | Linked to development of improvements | Degradation due to weight increase | Very mobile with engine upgrades, suspension, tires |
| **Range** | 35 km | Improved cannon and munitions | Increased testing at longer ranges | Increased performance with improved warheaads | 55-70 km range |
| Rate of Fire | T - 4 rounds/min for unguided<br>O – 6 rounds/min | Increases with each element | Increased testing time to prove out increased rate | Increased ability to service targets from less platforms | 8 rds/min…claims of 15-20 rds/min |
| Ammunition Storage | T/O – 39 rounds | No increased cost | | | 50-70 rounds |
| Embedded Training | On-board embedded tng | Factor in cost to maintain | Increased testing | Consider if actually used | No embedded training |
| Degraded Operations | Ability to engage targets in manual mode | $No additional cost – using modified chassis | Increased test time | Reduced crew members could impact | Degraded operation capable |

***Thresholds aren't "stretch" goals—must be achievable in time/money***

# When Requirements to Specifications is Easy



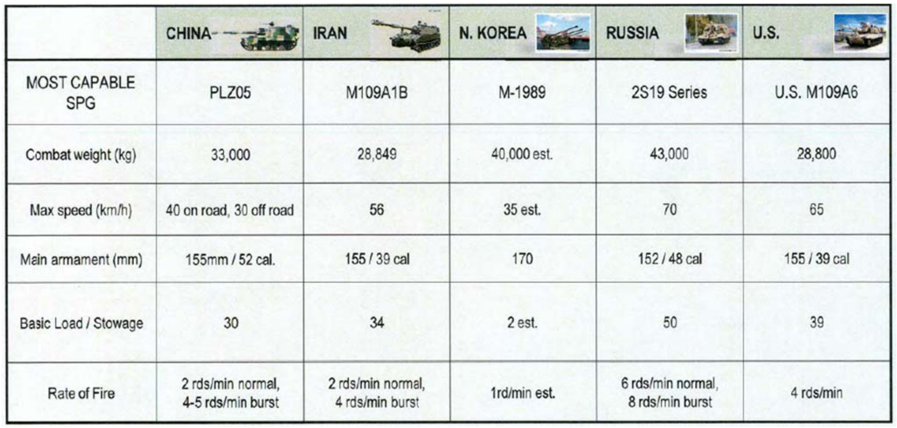


Key performance parameter.

- T: Range of 40 km; O: 70 km
- Stow 39 rounds
- Rate of fire: 4 rds per min

Engineering specification.

- T: Range of 40 km; O: 70 km
- Stow 39 rounds
- Rate of fire: 4 rds per min



| | CHINA | IRAN | N. KOREA | RUSSIA | U.S. |
|---|---|---|---|---|---|
| MOST CAPABLE SPG | PLZ05 | M109A1B | M-1989 | 2S19 Series | U.S. M109A6 |
| Combat weight (kg) | 33,000 | 28,849 | 40,000 est. | 43,000 | 28,800 |
| Max speed (km/h) | 40 on road, 30 off road | 56 | 35 est. | 70 | 65 |
| Main armament (mm) | 155mm / 52 cal. | 155 / 39 cal | 170 | 152 / 48 cal | 155 / 39 cal |
| Basic Load / Stowage | 30 | 34 | 2 est. | 50 | 39 |
| Rate of Fire | 2 rds/min normal,<br>4-5 rds/min burst | 2 rds/min normal,<br>4 rds/min burst | 1rd/min est. | 6 rds/min normal,<br>8 rds/min burst | 4 rds/min |

# GPS and Comms Jammers

•US/NATO reliance on GPS pervasive and growing
•Technology modest in cost but effective
➢Jamming inexpensive compared to anti-jam protection
•Good example of asymmetric warfare
➢Wide frequency coverage, high power
➢Multitasking: GPS, cell phones, multi-channel radio relay
High cost and complexity usually limit total numbers deployed

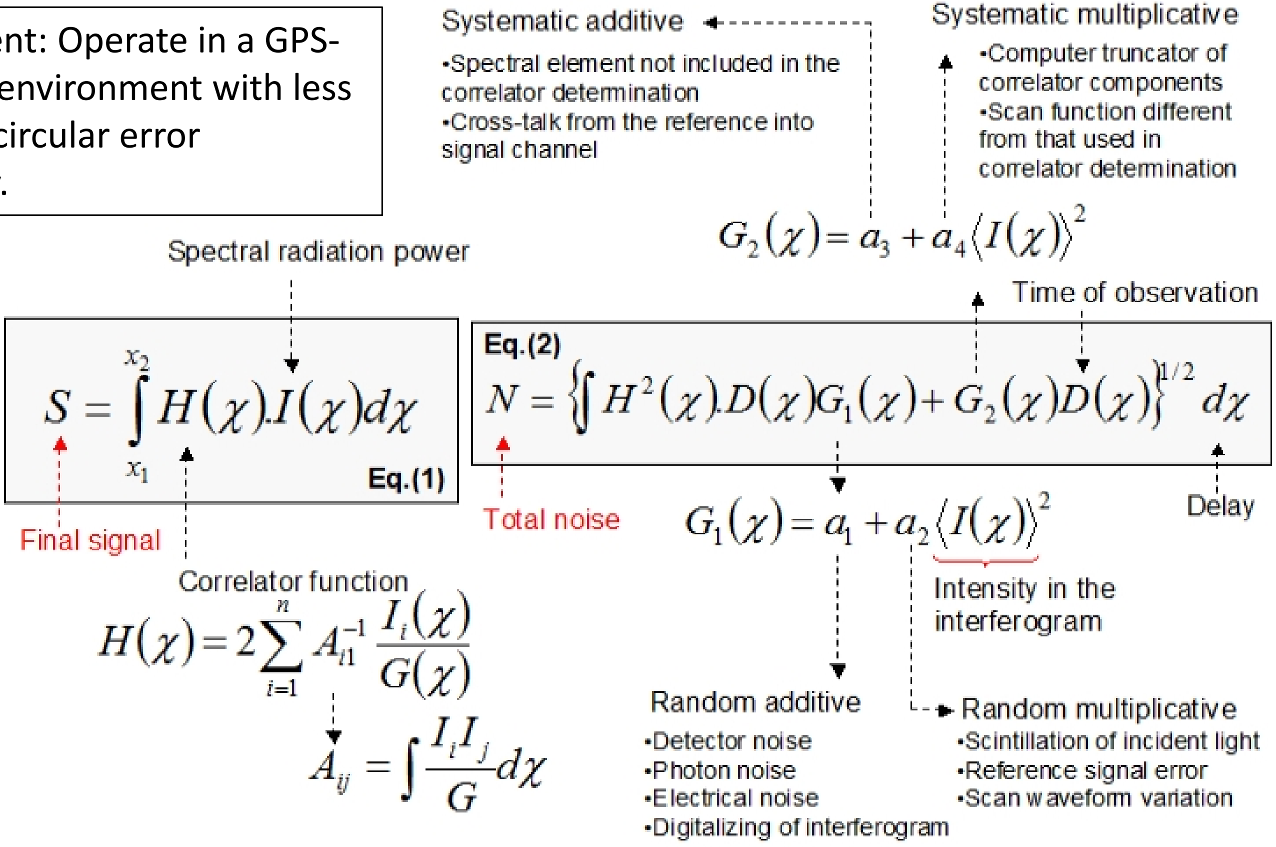
**WF-K6**
➢ 5 watt
➢ 4G 6 bands High Power

**TRC 274**
➢1-3000 MHz
➢Multi-mode, spot jamming, Smart Chirp

**Aviaconversiya III**
➢8 watt
➢Portable, lightweight
➢Claimed effective against US GPS and Russian GLONASS

# When Requirements to Specifications is NOT so Easy…

Requirement: Operate in a GPS-contested environment with less than 10m circular error probability.



Systematic additive

- Spectral element not included in the correlator determination
- Cross-talk from the reference into signal channel

Systematic multiplicative

- Computer truncator of correlator components
- Scan function different from that used in correlator determination

$$G_2(\chi) = a_3 + a_4\langle I(\chi)\rangle^2$$

Spectral radiation power

Time of observation

$$S = \int_{x_1}^{x_2} H(\chi).I(\chi)d\chi$$

Eq.(1)

Final signal

Correlator function

Eq.(2)

$$N = \left\{\int H^2(\chi).D(\chi)G_1(\chi) + G_2(\chi)D(\chi)\right\}^{1/2} d\chi$$

Total noise

Delay

$$G_1(\chi) = a_1 + a_2\underbrace{\langle I(\chi)\rangle}_{\text{Intensity in the interferogram}}^2$$

$$H(\chi) = 2\sum_{i=1}^{n} A_{i1}^{-1}\frac{I_i(\chi)}{G(\chi)}$$

$$A_{ij} = \int \frac{I_i I_j}{G} d\chi$$

Random additive

- Detector noise
- Photon noise
- Electrical noise
- Digitalizing of interferogram

Random multiplicative

- Scintillation of incident light
- Reference signal error
- Scan waveform variation

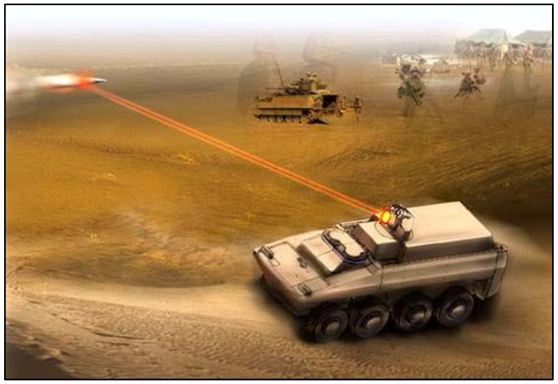
[1] J. Mattson, H. Mark, Jr., H. MacDonald Jr., Infrared, correlation and Fourier Transform Spectroscopy; In Computers in Chemistry and Instrumentation, Marcel Dekker Inc. New York, 1977, New York, pp. 1 – 233.

Performance specification:

GPS Anti-jam Performance
Under jamming conditions; the GPS receiver/antenna shall be capable of providing 20 dB J/S during a direct P(Y) acquisition and 35 dB J/S during aided track in the operating environment.

# Radiofrequency Weapon Threat

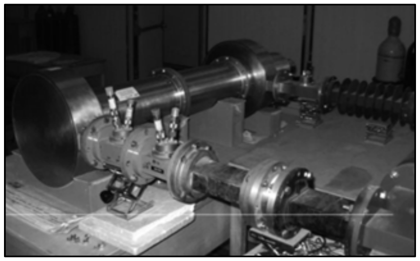
The Ranets E is a High Power Microwave (HPM) weapon system intended to produce electrically lethal damage or disruption and dysfunction in opposing airborne systems, be they aircraft or guided munitions in flight. The system was first disclosed by Rosoboronexport in 2001, but little technical detail has been disclosed since then. The weapon uses an X-band pulsed 500 MegaWatt HPM source, generating 10 to 20 nanosecond pulses at a 500 Hz PRF, and average output power of 2.5 to 5 kiloWatts. The antenna is large enough to provide a gain of 45 to 50 dB in the X-band. The weapon has been described as a **"radio-frequency cannon"**. Russian sources credit it with a lethal range of 20 miles against the electronic guidance systems of PGMs and aircraft avionic systems.



•Weapons that radiate strong electromagnetic pulses for the purpose of attacking electronic targets.

•Related terminology:

- Directed Energy Weapon – lasers, particle beams, RFW
- High Power Microwave—synonymous with RFW but higher frequency beam weapons
- Ultra-Wideband—EMP with very broad frequency content
- Non-Nuclear EMP—synonomous with RFW but contrasting with nuclear EMP



For over 6 years, Huang Wenhua and his team at the Northwest Institute of Nuclear Technology in Xi'an have been working on a potent microwave weapon. This one, which recently won China's National Science and Technology Progress Award, is small enough to fit on a lab work bench, making it theoretically portable enough for land vehicles and aircraft.

2018 2025 2035

# When Requirements to Specifications is NOT so Easy…

Requirement:

Must operate throughout the world-wide electromagnetic environment, including shipboard, without affect or disturbance to flight critical functions.

MIL-STD-464C: Electromagnetic Environmental Effects Requirements for Systems

- Specifies EM environment that systems' operational performance requirements are met.
- Includes all sources of EM radiation including RFW

Examplar

Performance specification:

Rotary Wing Aircraft including UAVs operating in 8000-8400 MHz, X-Band 7430 V/m – rms peak.

What are the operational ranges given the most likely and most capable threat?

- ➢ Drives hardening and cost
- ➢ Most likely – 5 km
- ➢ Most capable – 30 km

What are the TTP implications?

- ➢ Impacts CONOPS

# Questions?