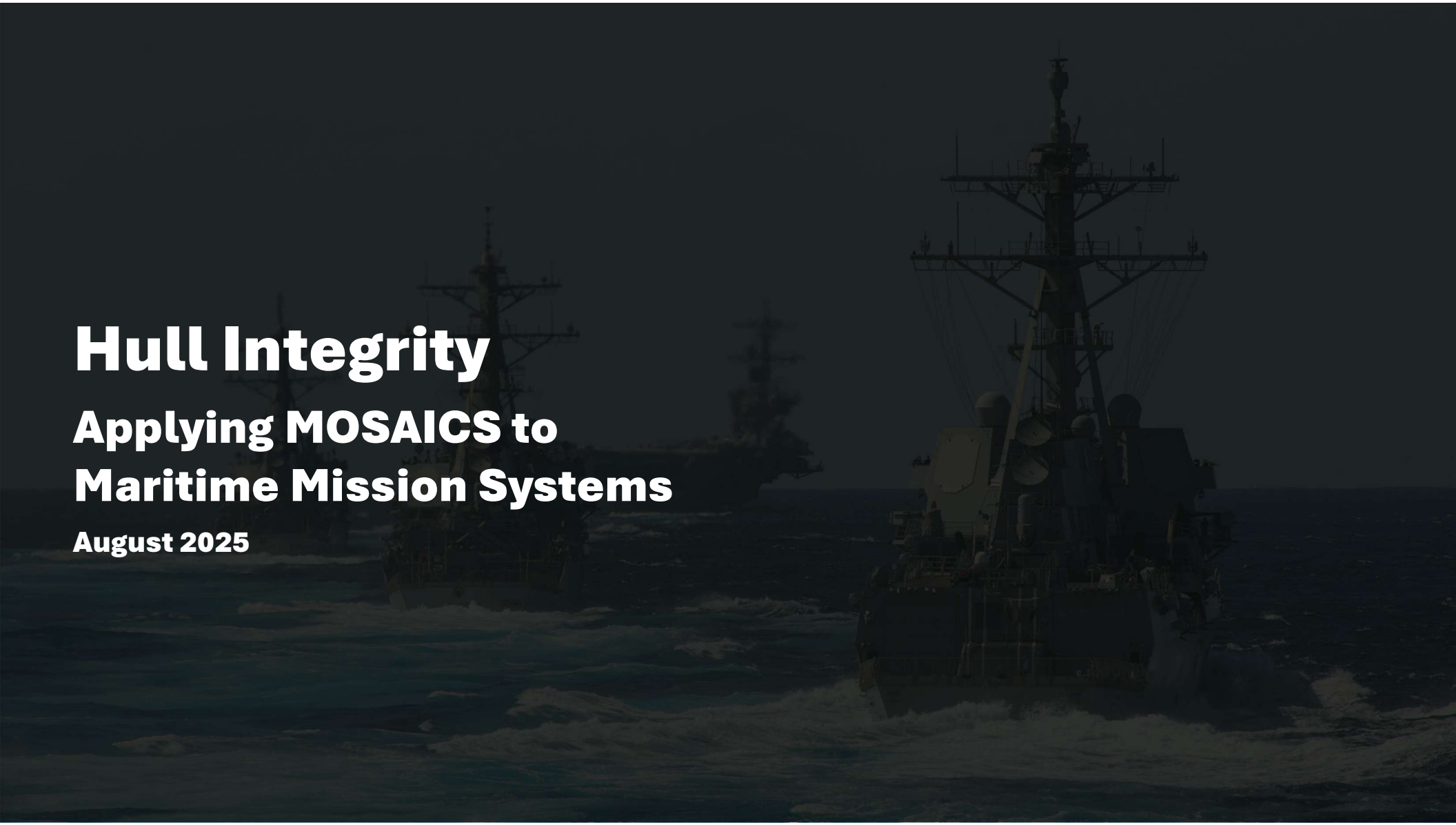


Hull Integrity

Applying MOSAICS to Maritime Mission Systems

August 2025



Mike Frank
Background and Experience

linkedin.com/in/mfrank174/

Department of the Navy
Deputy Chief Technology Officer

United States Marine Corps
Cyber Portfolio Lead - Marine Innovation Unit
Defensive Cyber Operations Bravo Company

Boston Consulting Group
Principal in the Tech and Digital Advantage practice

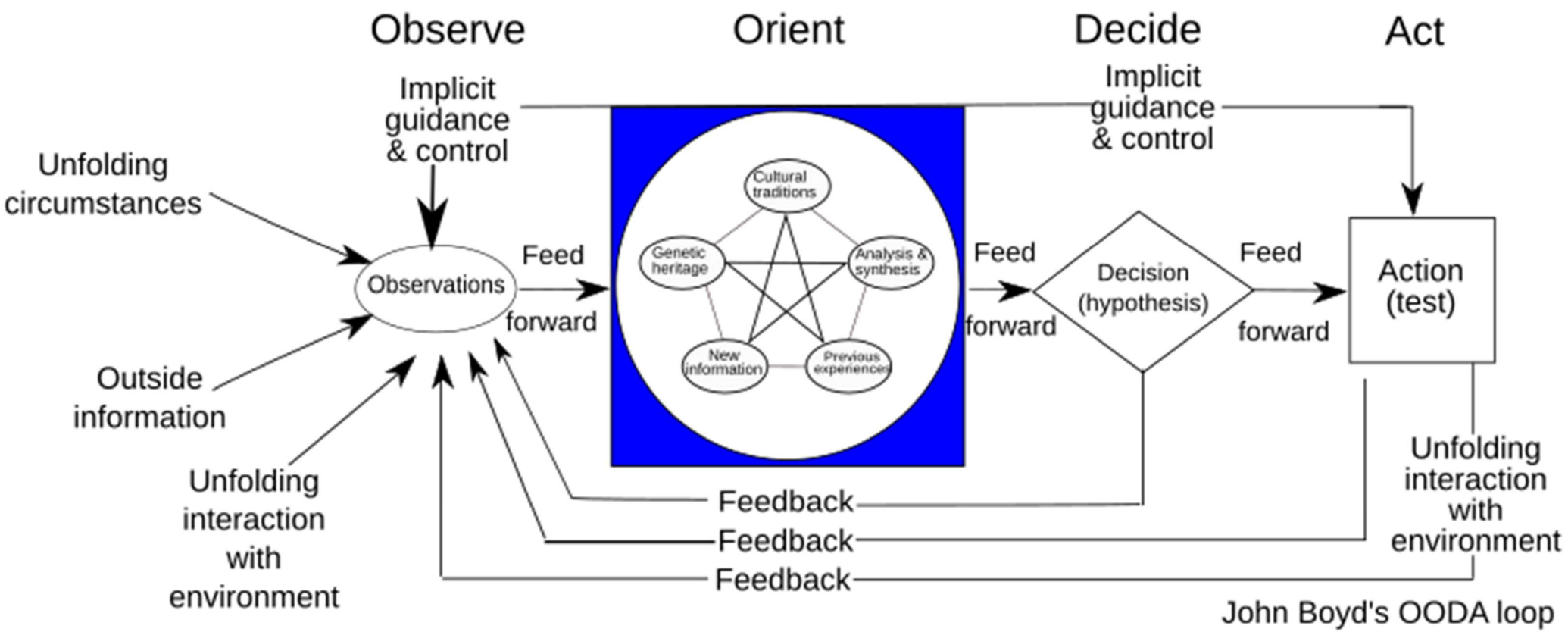
Accenture
Cybersecurity Strategy and Compliance Manager

Education
Carnegie Mellon University – MS, Cybersecurity
UVA Darden – MBA

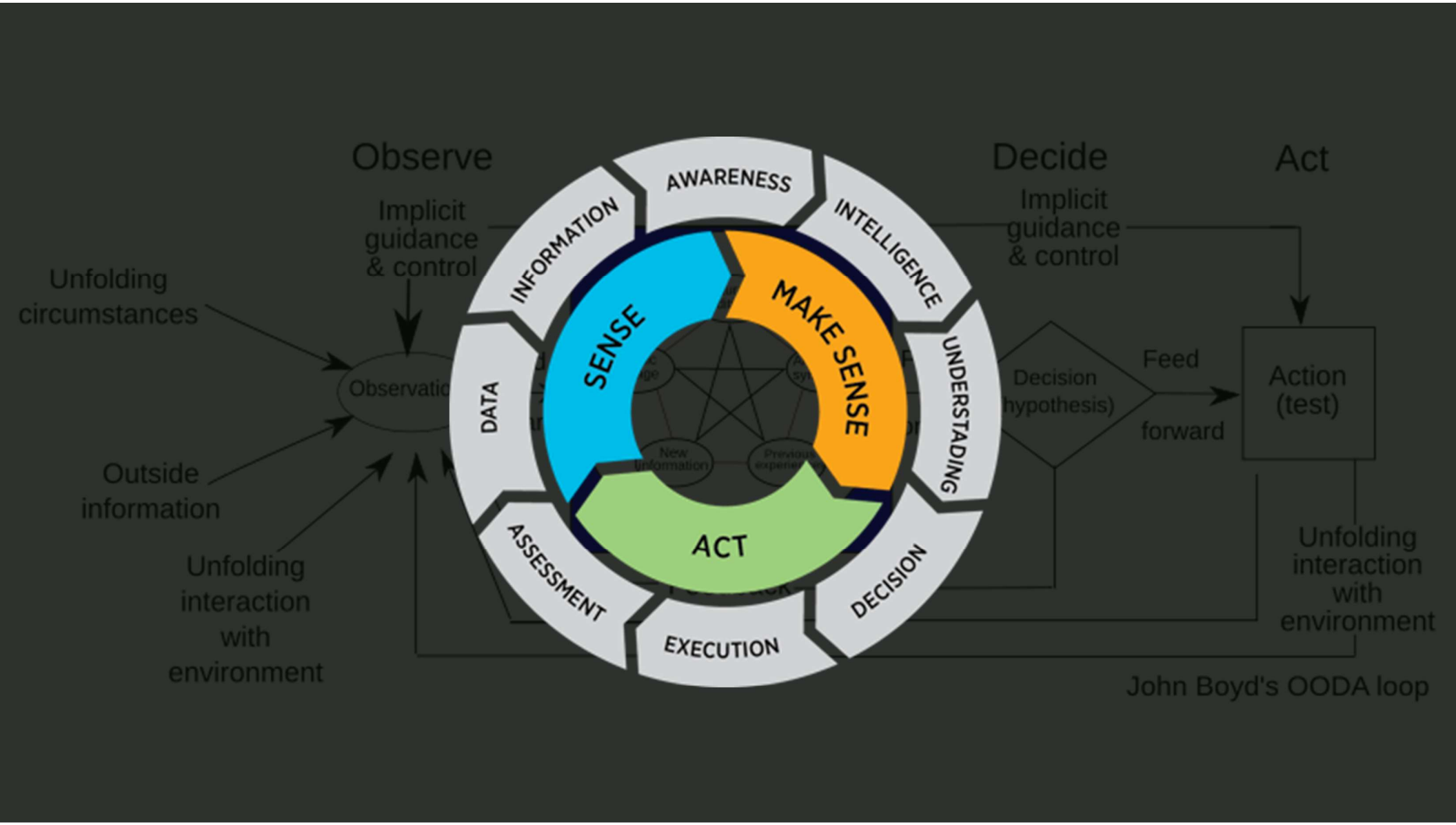
“Those who can handle the quickest rate of change survive”

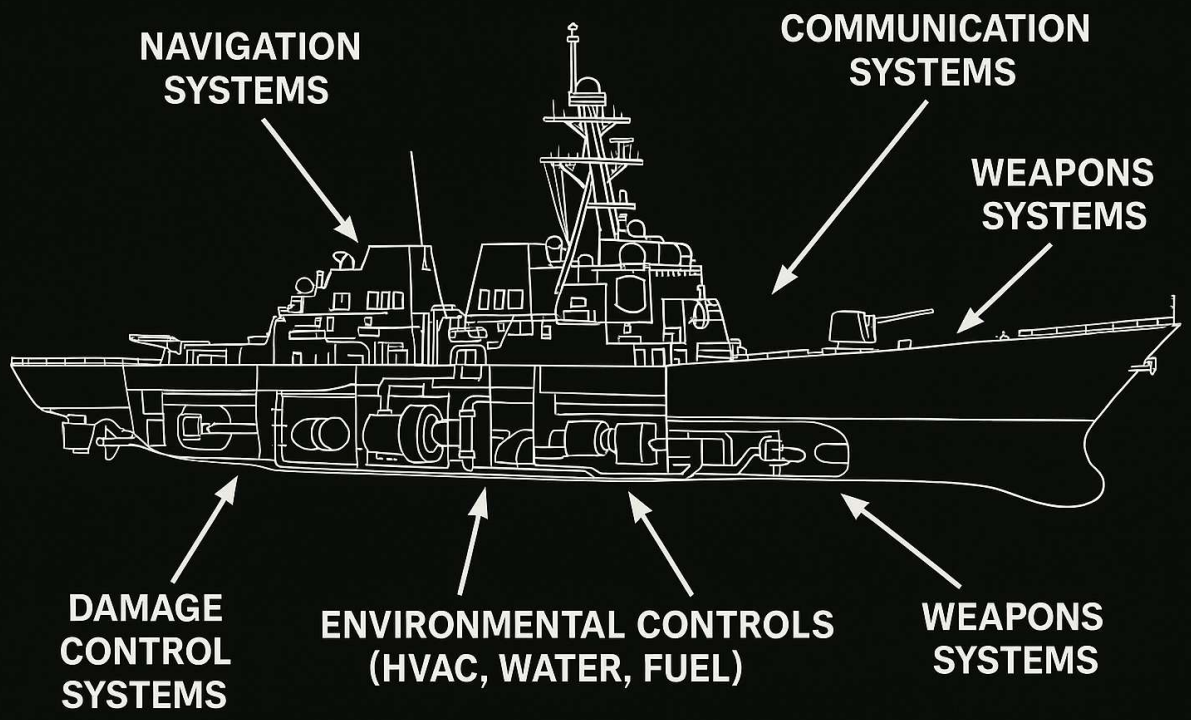
Colonel John Boyd, USAF

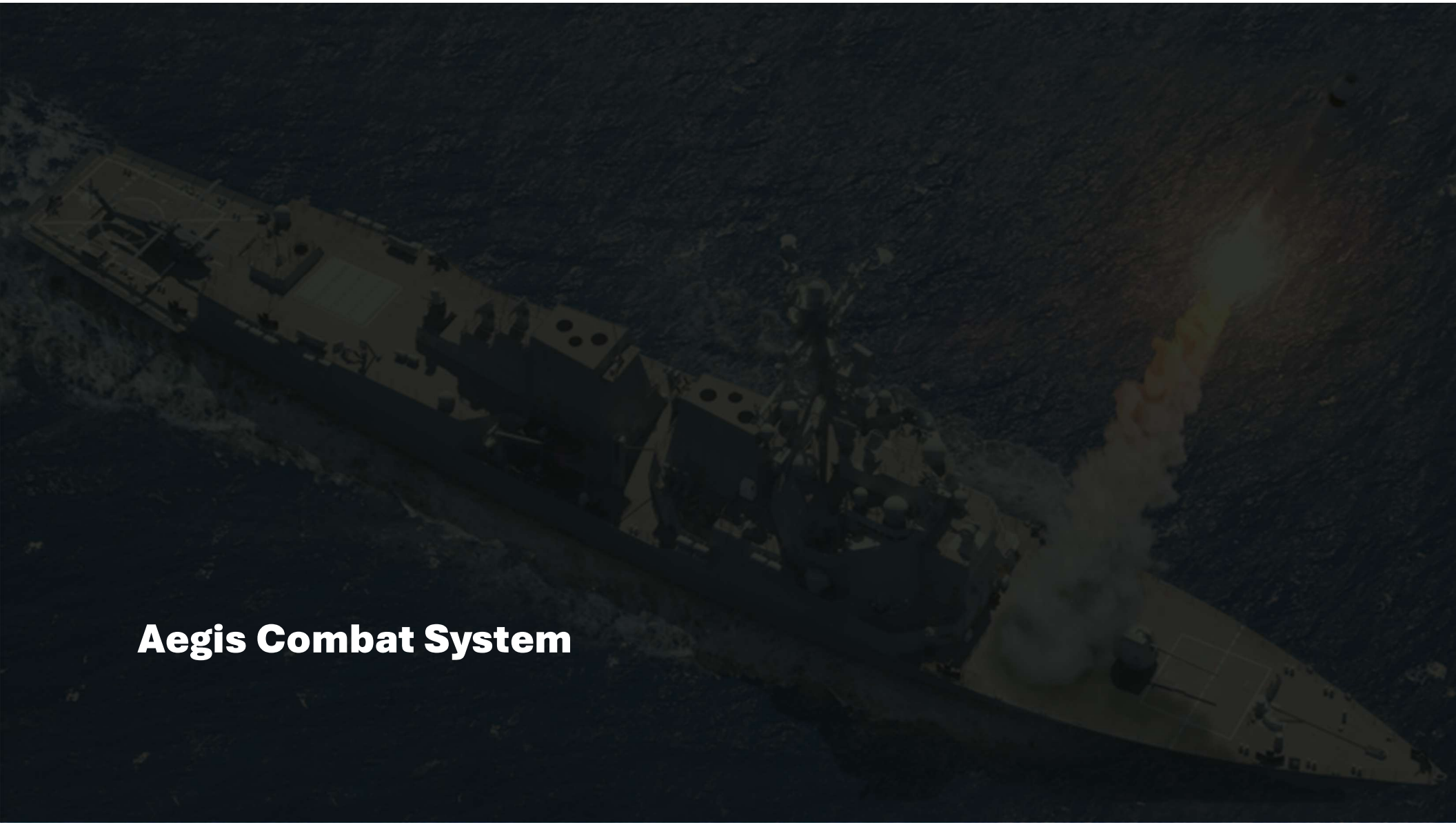




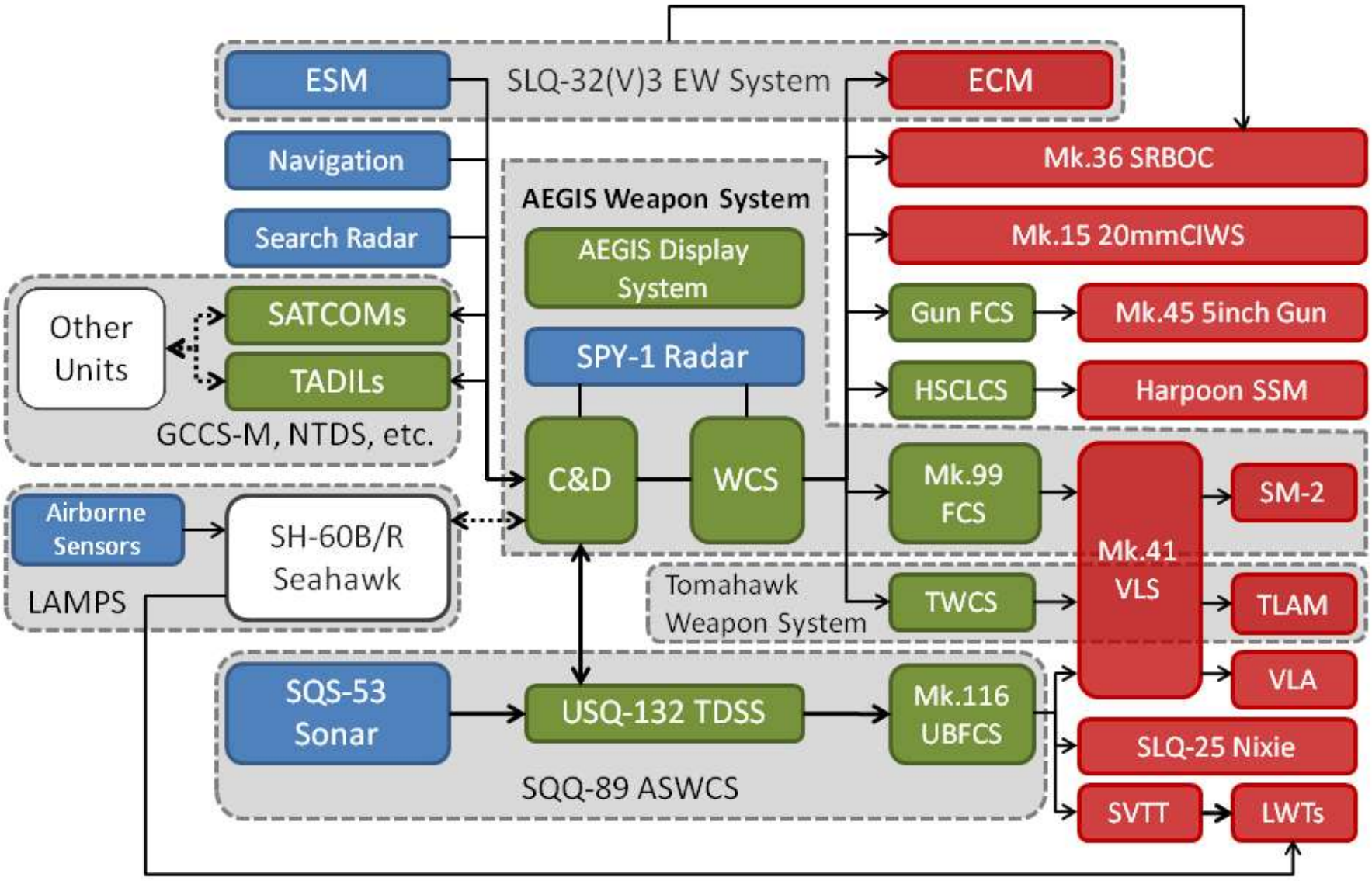
John Boyd's OODA loop

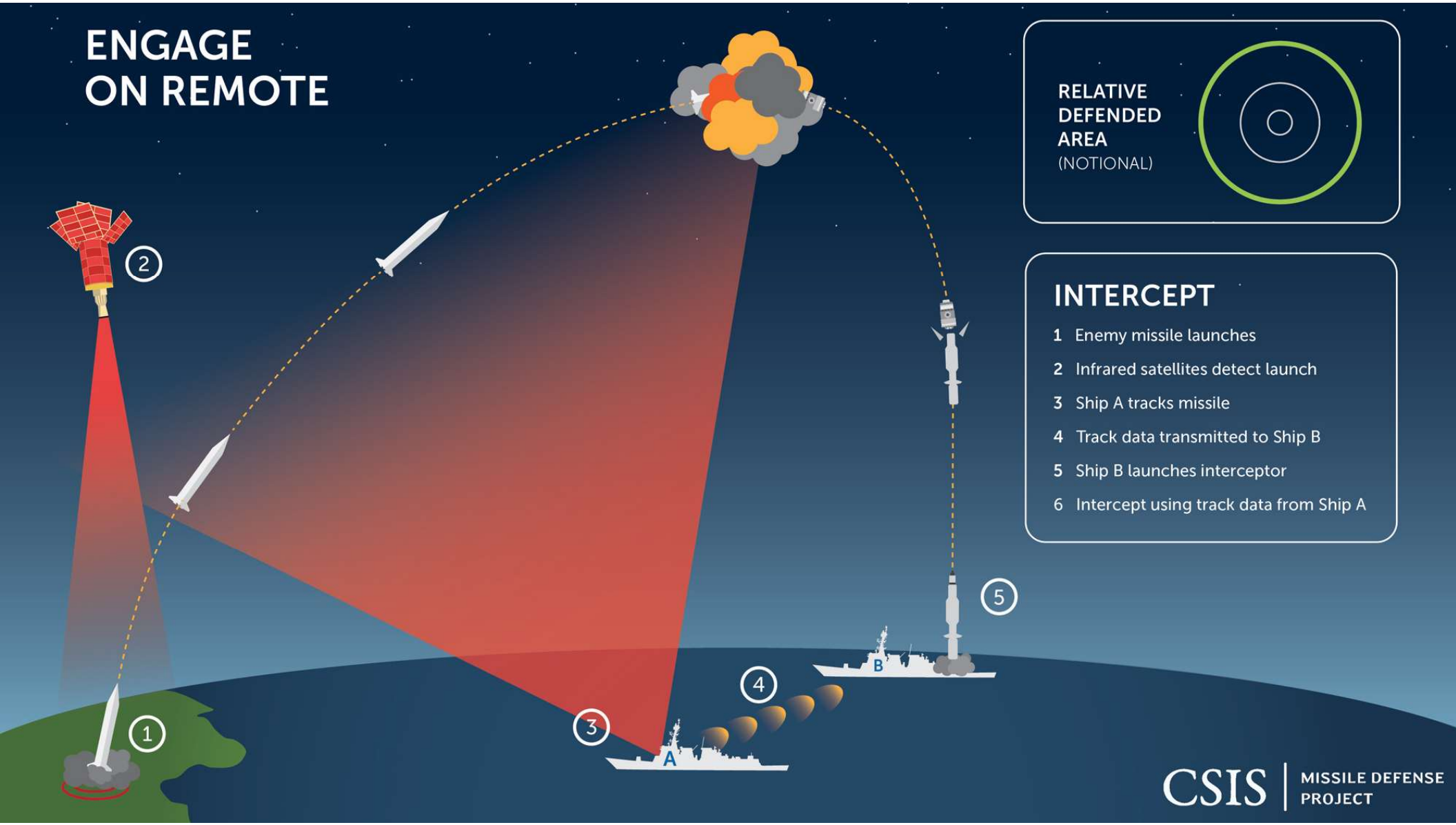

Observe
Decide
Act
Implicit guidance & control
Implicit guidance & control
Unfolding circumstances
Outside information
Unfolding interaction with environment
Observation
Decision (hypothesis)
Feed forward
Action (test)
Unfolding interaction with environment
AWARENESS
INTELLIGENCE
UNDERSTADING
DECISION
EXECUTION
ASSESSMENT
DATA
INFORMATION
SENSE
MAKE SENSE
ACT
New information
Previous experience
John Boyd's OODA loop

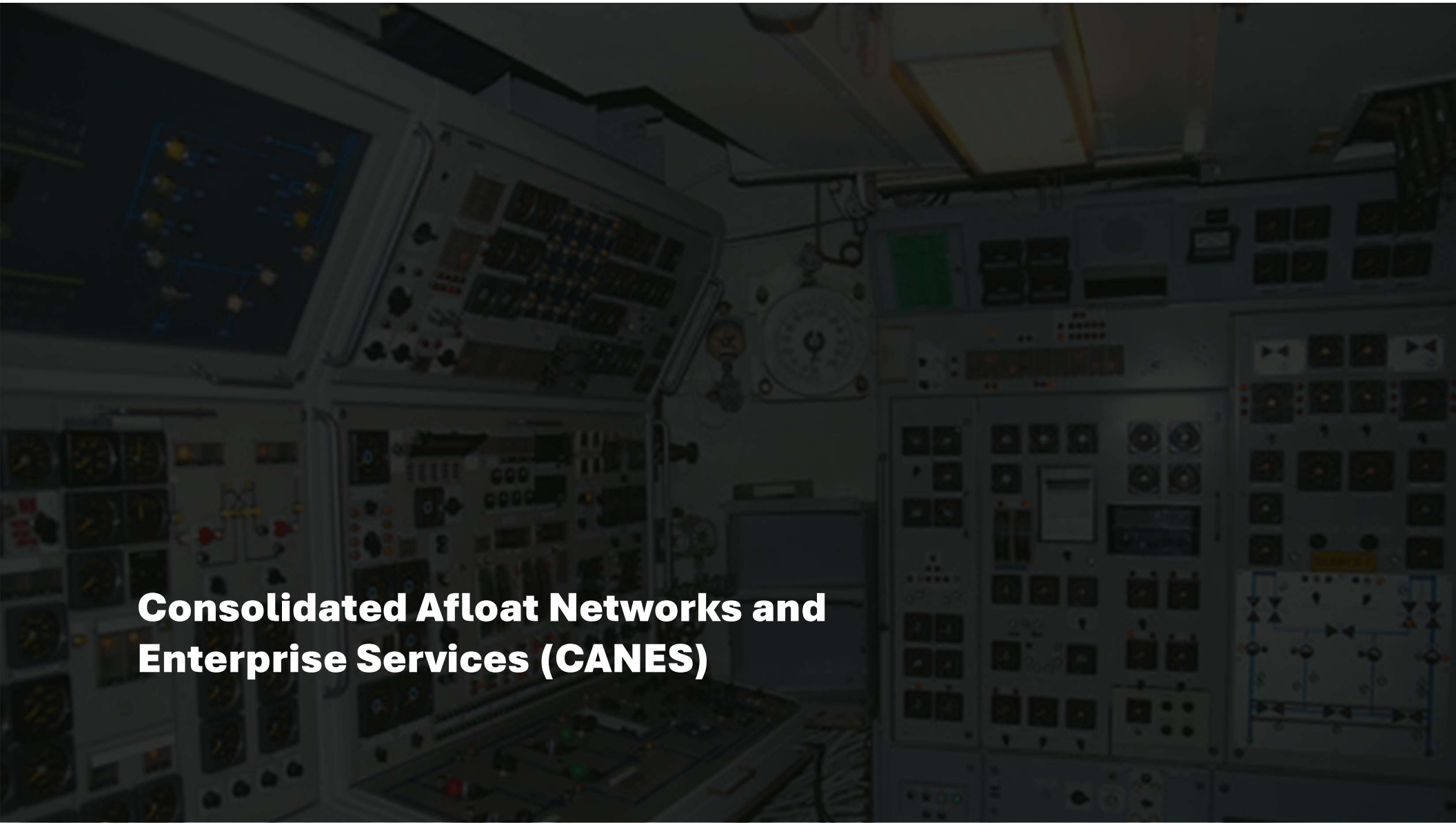

NAVIGATION SYSTEMS
COMMUNICATION SYSTEMS
WEAPONS SYSTEMS
DAMAGE CONTROL SYSTEMS
ENVIRONMENTAL CONTROLS (HVAC, WATER, FUEL)
WEAPONS SYSTEMS



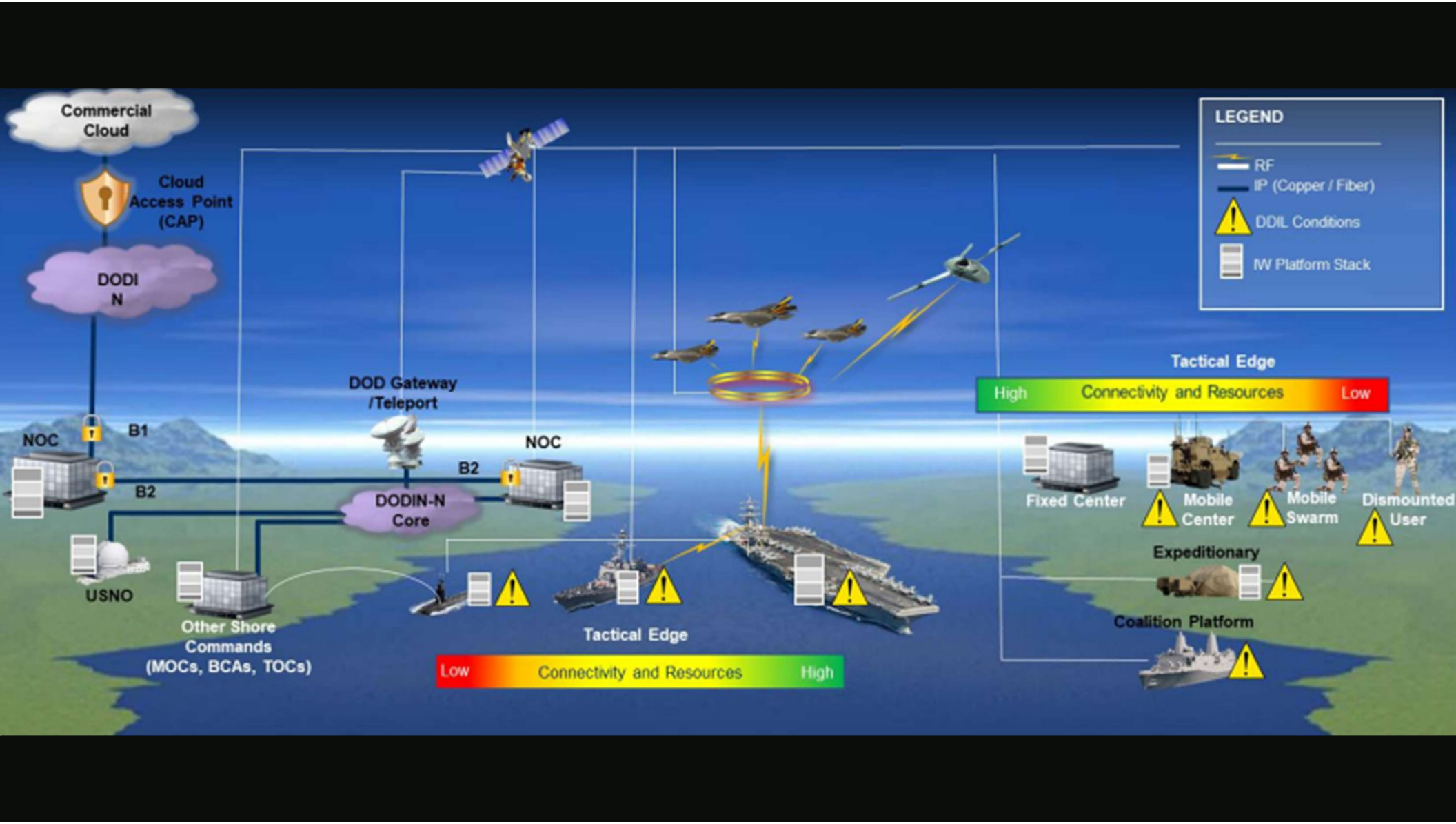
Aegis Combat System

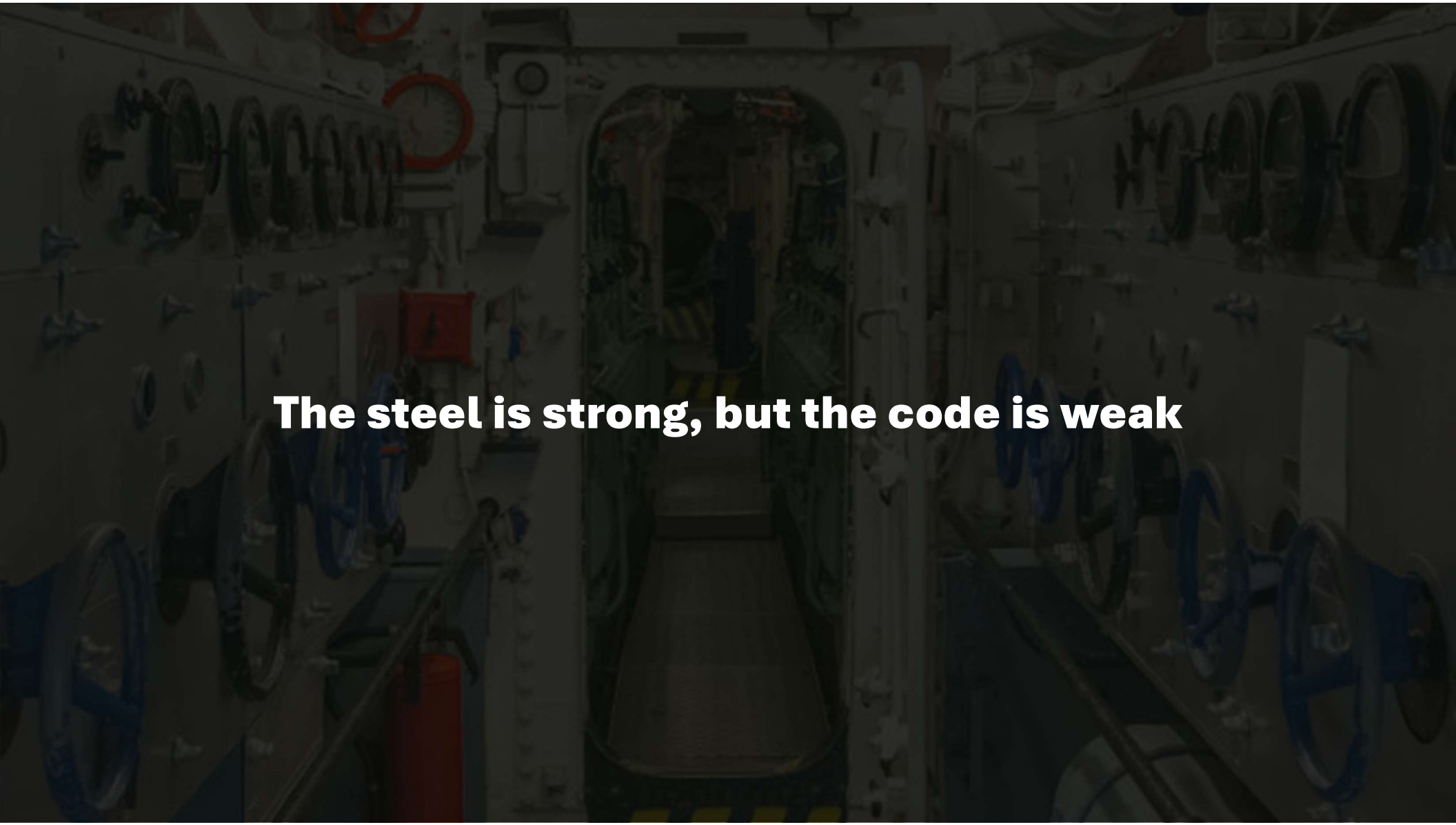

ESM
SLQ-32(V)3 EW System
ECM
Navigation
Mk.36 SRBOC
AEGIS Weapon System
Search Radar
Mk.15 20mmCIWS
AEGIS Display System
Other Units
SATCOMs
Gun FCS
Mk.45 5inch Gun
SPY-1 Radar
TADILs
HSCLCS
Harpoon SSM
GCCS-M, NTDS, etc.
C&D
WCS
Mk.99 FCS
Mk.41 VLS
SM-2
Airborne Sensors
SH-60B/R Seahawk
Tomahawk Weapon System
TWCS
TLAM
LAMPS
VLA
SQS-53 Sonar
USQ-132 TDSS
Mk.116 UBFCS
SLQ-25 Nixie
SVTT
LWTs
SQQ-89 ASWCS


ENGAGE
ON REMOTE
RELATIVE
DEFENDED
AREA
(NOTIONAL)
INTERCEPT
1 Enemy missile launches
2 Infrared satellites detect launch
3 Ship A tracks missile
4 Track data transmitted to Ship B
5 Ship B launches interceptor
6 Intercept using track data from Ship A
1
2
3
4
5
A
B
CSIS | MISSILE DEFENSE PROJECT



Consolidated Afloat Networks and Enterprise Services (CANES)


Commercial Cloud
Cloud Access Point (CAP)
DODI N
DOD Gateway /Teleport
NOC
B1
B2
B2
NOC
DODIN-N Core
USNO
Other Shore Commands (MOCs, BCAs, TOCs)
Tactical Edge
Low
Connectivity and Resources
High
LEGEND
RF
IP (Copper / Fiber)
DDIL Conditions
IW Platform Stack
Tactical Edge
High
Connectivity and Resources
Low
Fixed Center
Mobile Center
Mobile Swarm
Dismounted User
Expeditionary
Coalition Platform


The steel is strong, but the code is weak

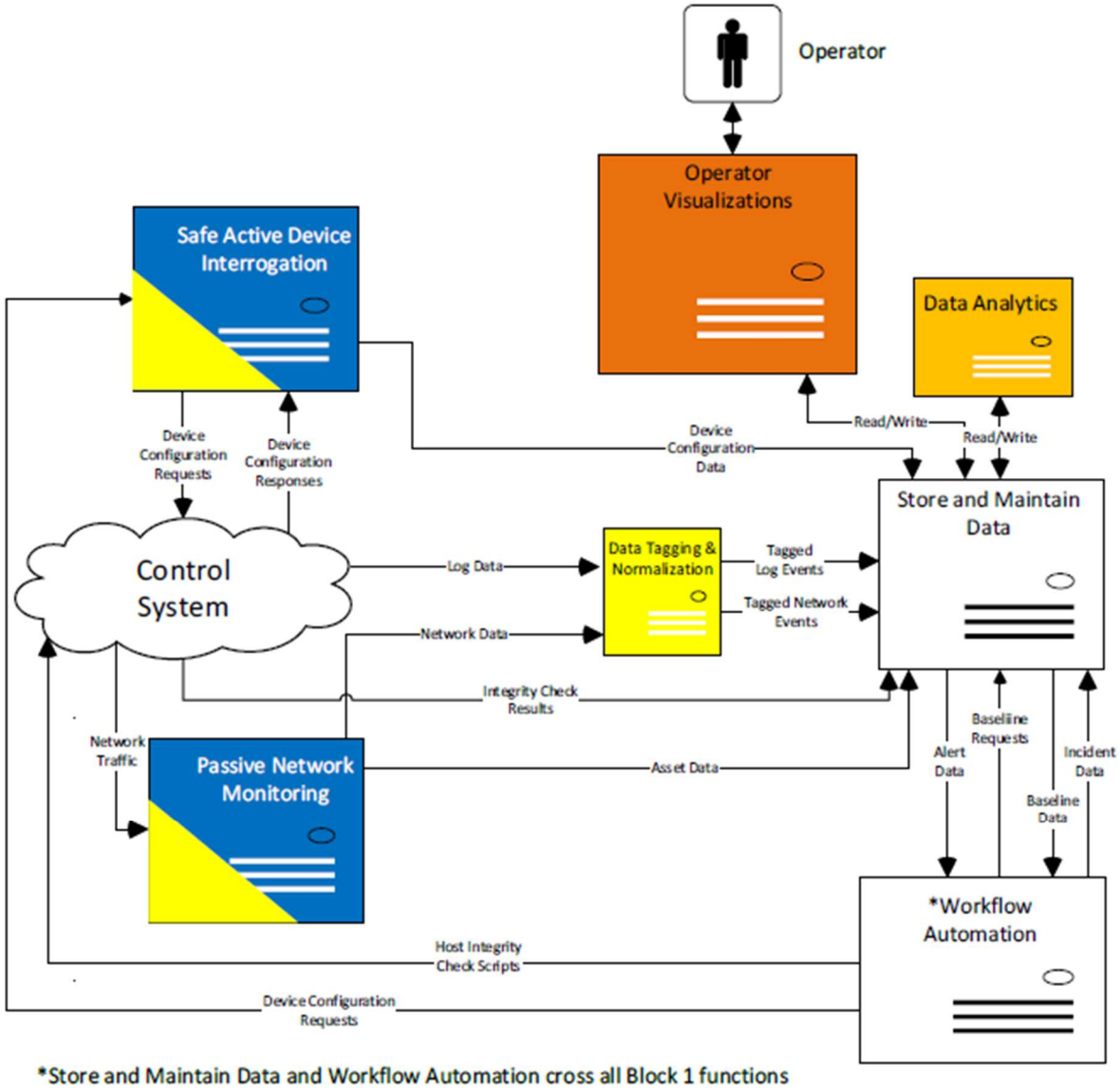


More Situational Awareness for Industrial Control Systems (MOSAICS)

A Department of Defense (DoD) effort to modernize the detection and response to threats to Industrial Control Systems

MOSAICS builds on itself to provide a comprehensive framework for defenders

Block	Sub-Block	Description	Capabilities
1	A*	Continuous passive monitoring of control system network and assets into a single data repository performing correlative analytics. Continuous collection of host event data, network intrusion detection alerts, network equipment logs, and network flow metrics.	- Aggregated asset inventory - Host monitoring - Network monitoring - Single aggregated event data repository - Behavioral aggregation analytics - Behavioral set correlation analytics - Visualization of events, alerts, and incidents
1	B*	Includes all functionality from Block 1A. Safe active enumeration of control system network and assets. Workflow management of a system baseline and on-demand integrity checking of control system assets against stored system baseline.	- All Block 1A Capabilities - Safe active enumeration of assets - Integrated system baseline creation - Automated workflow management for baseline creation and alert investigation - Host investigation with integrity checks
2	A	Includes all functionality from Block 1B. Workflow management of a system baseline and on-demand integrity checking of control system assets against stored system baseline. Automated generation of recommended courses of action, with automated execution of user-selected mitigations.	- All Block 1B Capabilities - Workflow automation for course-of-action suggestion - User-selected mitigation - Automated execution of user-selected mitigation actions
2	B	Includes all functionality from Block 2A. Bi-directional threat intelligence sharing between MOSAICS systems.	- All Block 2A Capabilities - Automated sharing of incident and mitigation details - Automated consumption and use of threat intelligence data
2	C	All functionality from Block 2B. Fine-grained response actions with follow-up recovery actions.	- All Block 2B Capabilities - Automated implementation of granular response actions - Automated execution of recovery actions



*Store and Maintain Data and Workflow Automation cross all Block 1 functions

The framework outlines a standard reference architecture for DON organizations to leverage

How do we make this work?

TOP 10 BEHAIVORS

Disrupt ourselves with **experiments**

Use before rent; rent before buy; buy before build

Beta earlier; a 10% solution is better than no solution

Partner bolder and as often as possible; leverage the success of others

Move with urgency and exercise a **bias toward speed**

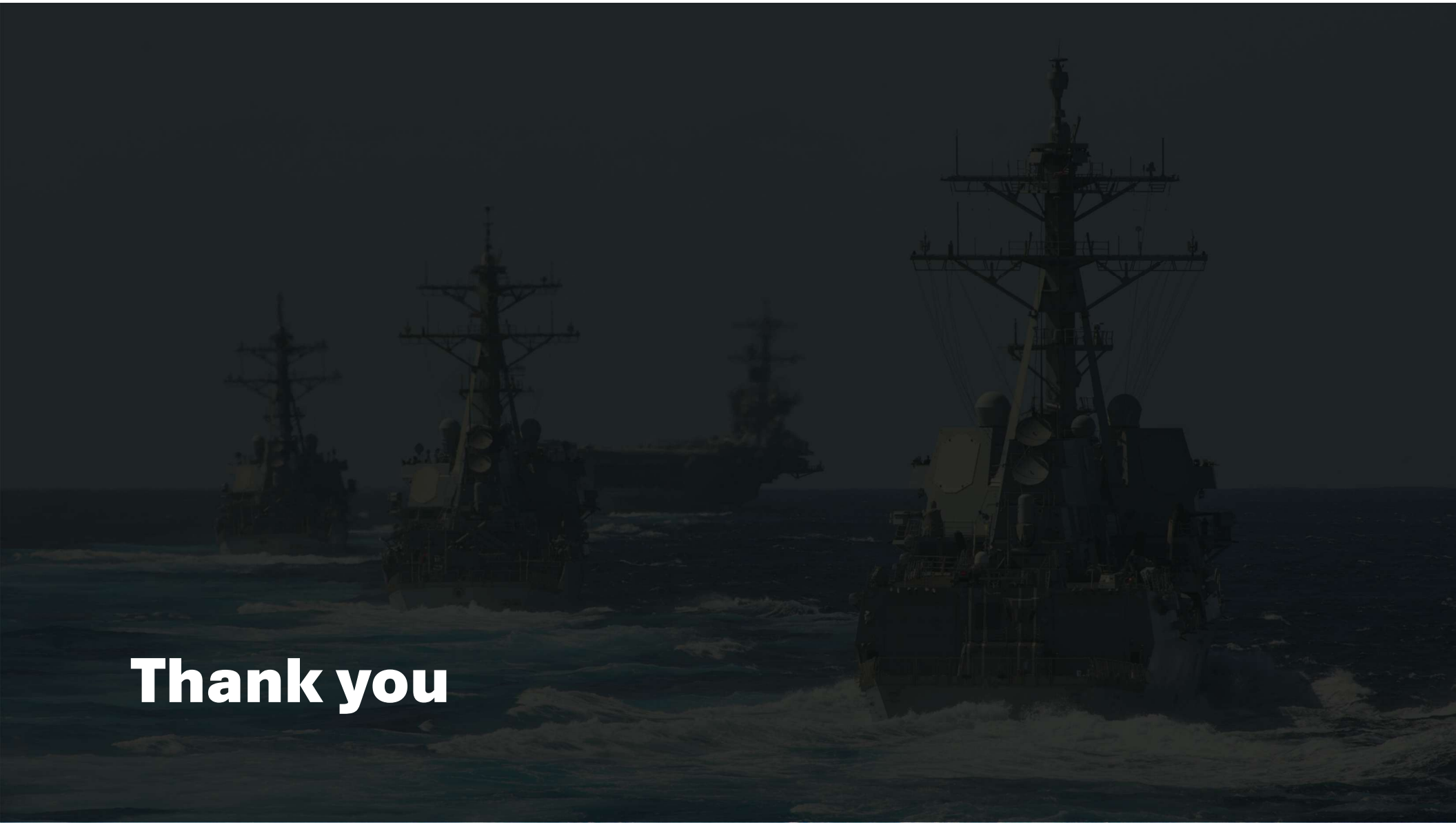
Seek **simplicity** for scalability

Seamlessly deliver **customer-centric** technologies

Never duplicate, **always automate**

Reward innovation; make government IT cool to do and boring to maintain

Weaponize data to make better decisions at the speed of relevance


Thank you