Maritime Cyber Security
"It's definitely a VUCA* environment"

Bob Day & Associates

* - Army War College 1990's

Maritime Cyber Security
“It’s definitely a VUCA environment”

Volatile

Maritime Cyber Security
“It’s definitely a VUCA environment”

Volatile

Uncertain

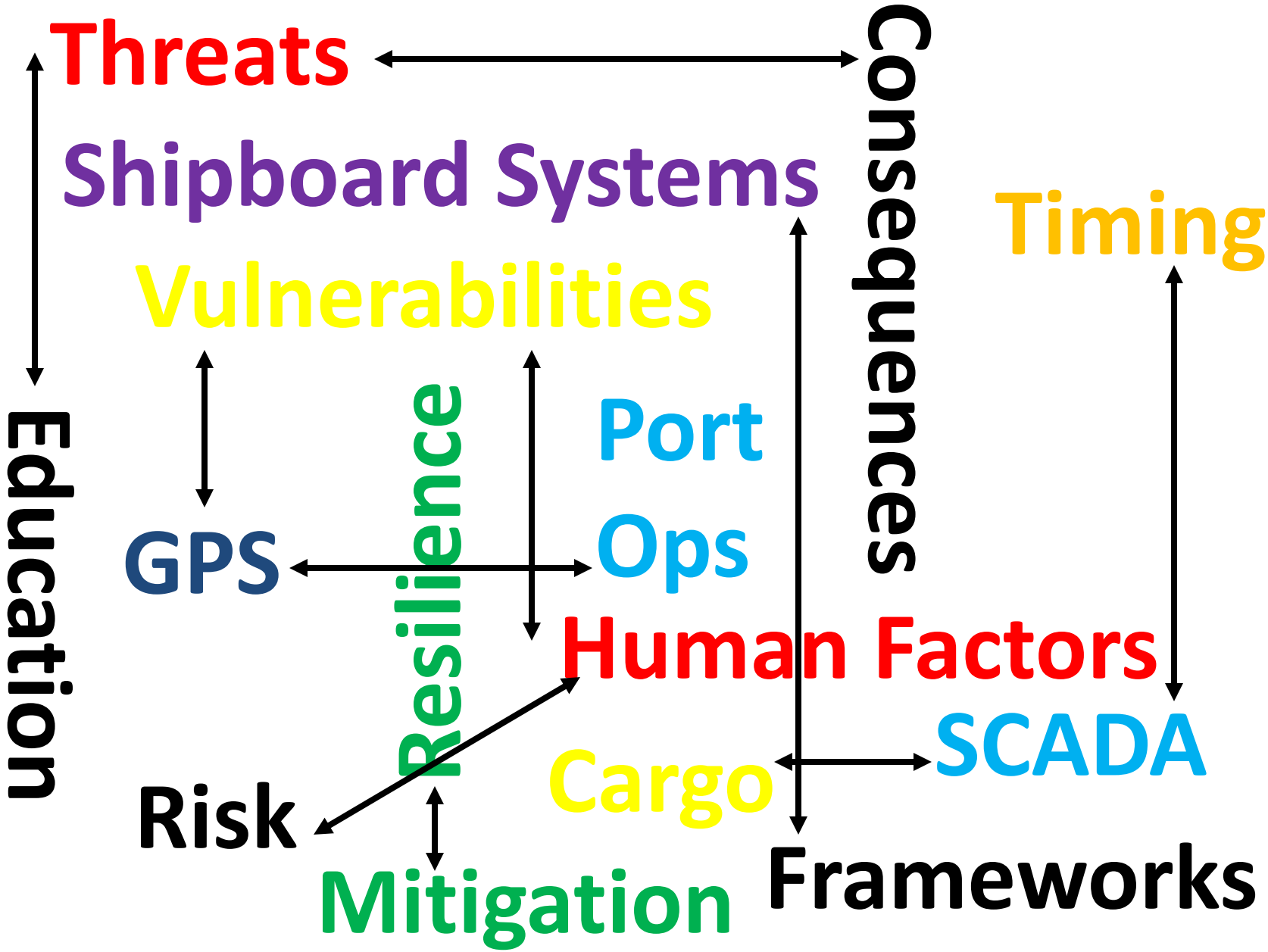
Maritime Cyber Security
“It’s definitely a VUCA environment”

Volatile
Uncertain
Complex

Maritime Cyber Security
“It’s definitely a VUCA environment”

Volatile
Uncertain
Complex
Ambiguous


Threats
Shipboard Systems
Vulnerabilities
Consequences
Timing
Education
GPS
Resilience
Port
Ops
Human Factors
SCADA
Cargo
Risk
Mitigation
Frameworks


Threats
Consequences
Shipboard Systems
Timing
Vulnerabilities
Education
Resilience
Port
GPS
Ops
Human Factors
SCADA
Cargo
Risk
Mitigation
Frameworks

To function in a VUCA environment organizations must:

- **Anticipate the Issues that Shape Conditions.**
- **Understand the Consequences of the Issues and Actions.**
- **Appreciate the Interdependence of Variables.**
- **Prepare for Alternative Realities and Challenges.**
- **Interpret and Address Relevant Opportunities.**

Based on the presentations and discussions during this event:

- **We are just beginning to understand the broad array of issues that impact this domain.**
- **We do not fully understand the potential consequences of the issues and actions that we might undertake.**
- **We do not fully understand the interdependence of the variables especially the impacts in other domains.**
- **We are far from developing strategies to operate in alternative/degraded environments.**
- **We, as a maritime community, need to interpret all of the above and develop comprehensive strategies to develop mitigations and improve resilience.**

Laying down a new track line!

- **Continued research and collaborative approaches to identify the core issues and ability to mitigate their impact.**

- **Leverage Risk Management Frameworks to begin to understand the consequences and prioritize the actions we undertake.**

- **Conduct broad reaching exercises to test our plans and fully understand the impacts in other domains and the supply chain.**

- **Leverage the above to enhance overall resilience of the MTS.**

Key way points!

- **Build the community and be inclusive. Fed, State, Public, Private, Industry, Supply Chain, and Academia. Look at what the financial community has done.**

- **Unfettered exchange of threat, impact, and mitigation information. Leverage existing architectures and evolving information exchange policies to overcome liability concerns.**

- **Develop and codify voluntary standards and best practices for all cyber aspects of the MTS. Certify third party entities to conduct assessments and certifications.**

- **Create and share best of class training/outreach programs.**

We are underway but need to turn a few more knots!

- **Leverage the information and contacts obtained from this event. Share broadly and engage others.**

- **Watch for, read, and share the forthcoming CG Cyber Strategy.**

- **Engage in local Area Maritime Security Councils, FBI InfraGard, and Maritime ISAC.**

Questions?