"The Nature of NextGen Military Networks"

NDIA Conference ■ 26 October 2015 ■ Springfield, VA.

Dr. S.S. Kamal

SAIC
Redefining Ingenuity™

SCOPE of Our Dialog

ABSTRACT: "The Nature of NextGen Military Networks

The relentless technology advances challenge military experts to stay ahead of the curve. Projecting force remains a critical U.S. National Security imperative; a vital tool to our global diplomatic efforts. Today's technology advances present unique challenges in that they demand rethinking the very nature of our military networks.

ACQUIRING INTEROPERABILITY

SECURING INTEROPERABILITY

ACQUIRING INTEROPERABILITY

WHY IS ACQUIRING INTEROPERABILITY A CHALLENGE?

1. We have the Joint Capabilities Integration and Development System (JCIDS)
2. We have the Joint Requirements Oversight Council (JROC)
3. We have Functional Capabilities Boards (FCBs)
4. We have the Defense Acquisition Board (DAB)

…and…..
once we have a formal ACQUISITION PROGRAM…..

5. We have a DAE
6. We have a MDA
7. We have a PM and PMO

ACQUISITION PROGRAM

INTEROPERABILITY is 1 of TOP 3 CHALLENGES!

A SYSTEMS PROBLEM?

- INTEROPERABILITY requires
  - Modularity → so things can scale to fit missions
  - Repeatable processes → so interoperability is reliable
  - Reuse → so DoD doesn't have to pay N times for marginal differences
  - Rigorous interoperability testing……Rigorous !!!

- None of these things fit programs that are planned to get from A→Z in the shortest time, at least cost. None of these fit LPTA

- Neither JCIDS documents, nor JROC directions, nor programs are structured for INTEROPERABILITY- SECURITY – AFFORDABILITY.

- Not a PROCESS problem….the SYSTEM DESIGN is weak.
  - Process Driven: The DAG Cookbook
  - Not insufficient oversight….weak oversight
  - Bad SE form: poor design documentation and testing during development

OUTLAW CUT-n-PASTE!

SECURING INTEROPERABILITY

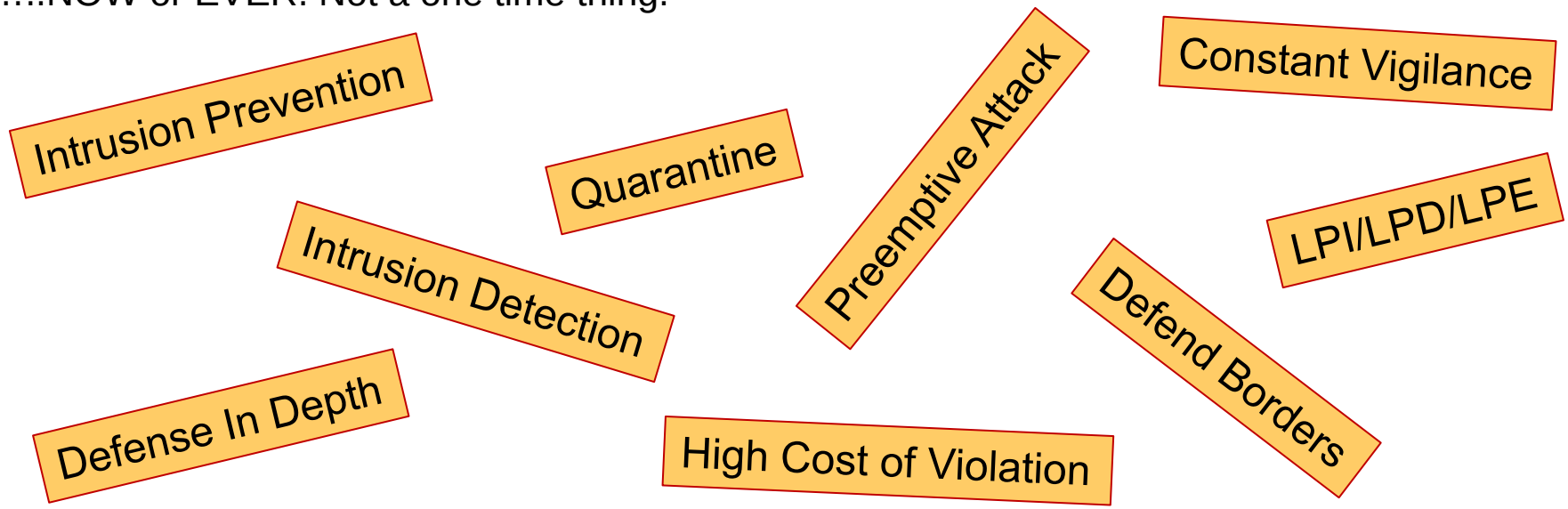
On the surface: an OXYMORON…..2 irreconcilable objectives.

- We want more information, faster, and everywhere…but…..
- We need to secure every border, every portal, every device, and every interface.
- Circle the wagons….but operate seamlessly!

SECURITY ≠ DEFENSE

SECURITY should be defined as **preventing mission objectives from being compromised**……

…..NOW or EVER. Not a one time thing.



A SYSTEM PROBLEM?

YES…BUT….

1. SECURITY Is not built into our programs
2. When it is….it is process driven

Exciting technologies are emerging in cyber security conferences & forums

- They are **COMPONENTS** of security
- How do we put them together in effective, secure systems?

THE OBVIOUS

1. We need to improve & simplify our existing processes
   - Less quantity and more quality
2. We need to train PMs like CEOs not Administrators
3. We need to hold PMs and PMO team accountable beyond their “rotation”
4. We need to structure smart programs that achieve

   INTEROPERABILITY SECURITY AFFORDABILITY

   Not preoccupied with “Achieving Milestone C”
5. We need to rediscover SE disciplines of design, test & documentation

…..and OUTLAW CUT-n-PASTE!

NextGen Military Networks

1. More devices and more complex software.
2. Increasing degrees of automation and cognition.
3. Where do we put the “human-in-the-loop”?
4. Support Coalition Forces…..with Coalition equipment.
5. Renounce doctrine of 2 simultaneous conflicts.
6. Not revolve around BIG DATA or DATA FUSION
7. Challenge how the military defines its requirements.
8. MORE Fragmented acquisition, not less.
9. Force organization restructured.
10. No tolerance margin for sloppy acquisition and security

Questions?

Dr. S.S. Kamal ■ Chief Scientist / Engineering ■ Phone: 858-967-0589
E-Mail: kamalss@saic.com ■ ssk@zooka.net