Aligning Information Assurance with Operational Need:
National Information Assurance Engagement Center

Wende Peters
wende.peters@jhuapl.edu

NIAEC

Today's DoD IA Reality

- Global Information Grid (GIG) demands new IA approaches
  - COTS protocols and software are not trustworthy
  - Widens the IA focus to availability and integrity as well as confidentiality
  - Vastly improves access for adversaries ("Power to the edge")
- Need for an immense, new Security Management Infrastructure
  - Universal, technology-based identification, authentication & authorization
  - Cryptographically bound security labels
  - Dynamic Identity & Privilege Management
  - Dynamic Coalition or Community-of-Interest Management
  - Attack Sensing and Warning
  - Attack reaction and service restoration
  - Attack traceback and response

NIAEC

Impact of the IA Paradigm Shift

- Some still fail to recognize the need
  - The magnitude of the threat is still closely held
  - The impact of most current attacks is not apparent
- Many recognize the need, but don't understand the technology
  - When is each technology applicable, and when is it not?
  - How do similar products offered by multiple vendors differ?
- More can't express their requirements
  - Disconnect between user and researcher perspective on CONOPS
  - Relative priority of availability, integrity and confidentiality
- Most fail to address the substantial gaps in current IA technology

Barriers to Bridging the Gaps

Risk goes unrecognized

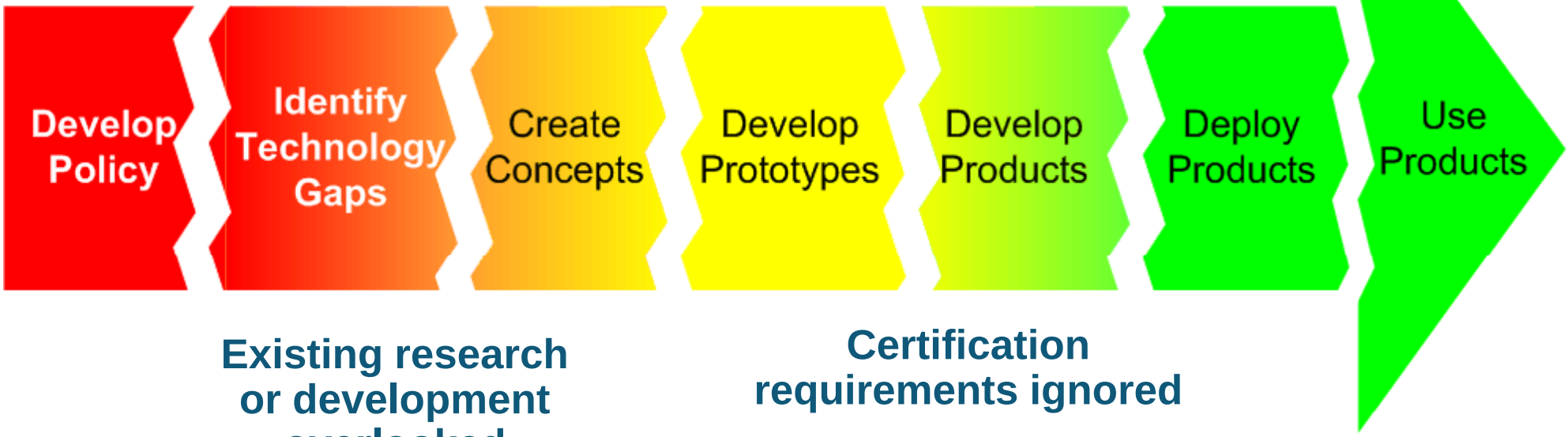
Potential/limitations of technology not understood

User requirements not understood

Users don't realize what is possible

Poor interfaces to protected systems

Mismatched interfaces between IA products



Existing research or development overlooked

Certification requirements ignored

Productization requirements ignored

Budget cycles missed

NIAEC

What is NIAEC?

A collaborative venture between NSA and JHU/APL that enables researchers, developers, Government decision-makers and users to explore, influence and expedite the fielding of emerging IA technologies

- NIAEC provides an immersive experience where IA solution providers, IA decision makers, operational users, and acquisition managers can engage regarding:
  - PAST: Lessons learned regarding operational needs and constraints, evaluation and certification processes, technology integration, deployment, maintenance and training
  - PRESENT: Best practices in technology use, configuration, operational deployment; the *art of the possible* with today's technology
  - FUTURE: Demonstration of emerging IA technology solution *in operational settings using operational systems*; Technology transition planning to aid transfer of technologies from researchers and developers to operational community

NIAEC Goals

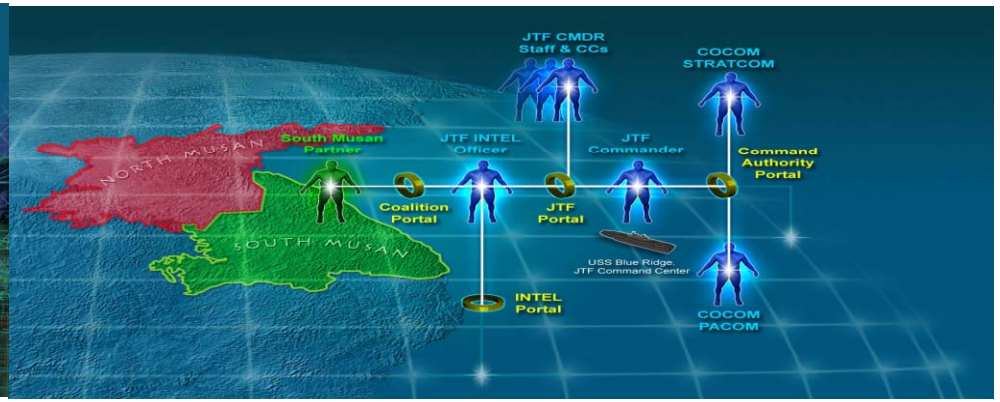
- **Educate**
  - Educate non-IA professionals about the potential and limitations of IA technology, as well as the risks mitigated by IA technology
  - Educate IA community, researchers, and developers about operational needs and constraints
- **Shape the future**
  - Highlight crucial technology investment areas for significantly improved IA
  - Introduce operational needs and constraints into IA research
- **Enhance technology transition**
  - Speed the process of fielding user- and threat-appropriate IA technology by bringing together participants
  - Demystify the transition process by defining a straw man transition plan for demonstrated technologies
  - Address early the full scope of transition considerations: technology maturation, evaluation and certification, acquisition and budget synchronization, and operational needs alignment

NIAEC

The NIAEC Demonstrations

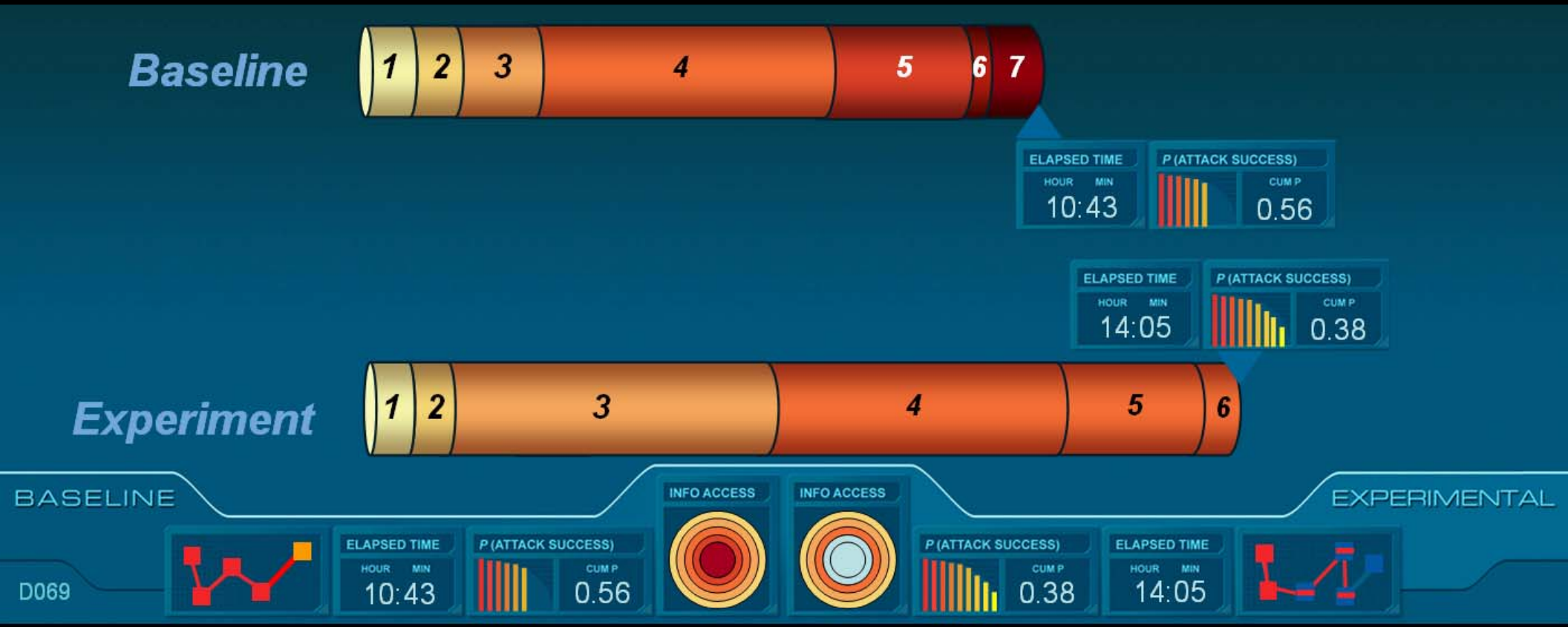
NIAEC Mission: ***Provide a forum for engagement among those who develop and operationally deploy IA solutions to enhance national security by moving IA technologies into the hands of warfighters***

- **Insert IA technologies into operational scenarios and realistic system configurations**
- **Demonstrate the effects and impacts in a realistic OPSIT**
- **Educate operational users on the abilities and benefits of emerging IA solutions**
- **Educate IA researchers on operational needs and likely employment scenarios**
- **Facilitate technology transition from researchers to programs of record**



NIAEC

NIAEC Attack Progression

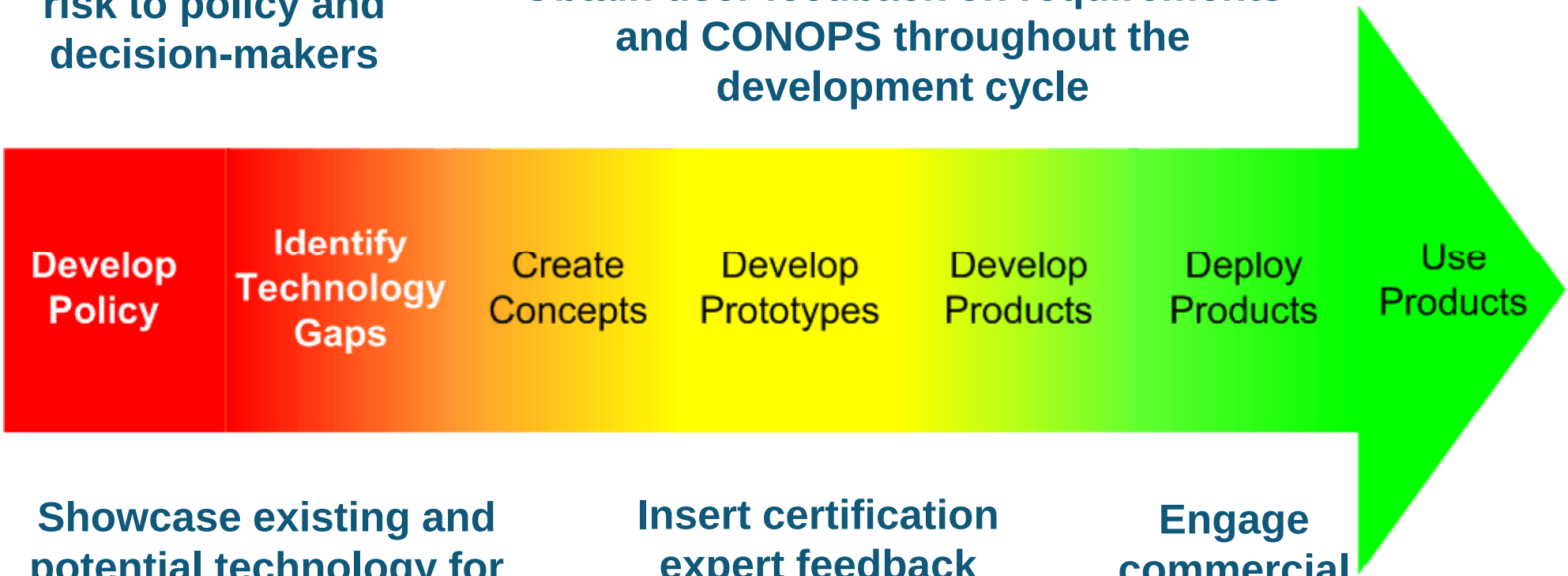


- Baseline attacker able to complete all attack steps and compromise most critical info
- Experimental attacker's network intrusion contained within partitions - unable to compromise past attack 4
- Baseline attacker had 56% likelihood to get all the way in
- Exp attacker contained to 38% likelihood of getting only part way – probability approaches zero for them getting most critical mission data

NIAEC: Aligning Operational Need with Technical Possibilities

Demonstrate the risk to policy and decision-makers

Obtain user feedback on requirements and CONOPS throughout the development cycle



Showcase existing and potential technology for acquisition decision-makers

Insert certification expert feedback throughout the development cycle

Engage commercial interests

NIAEC

NIAEC Operations

- Develop 1-2 major demonstrations per year
  - Prior technologies and demonstrations remain in the NIAEC portfolio
- Develop a rotating and evolving set of expositions and exhibits
  - Showcase best practices and recommended configurations
  - Lessons learned and IA educational materials
- Provide NIAEC demonstration and visits on an ongoing basis
  - Leverage APL relationships with programs of record
  - Include NIAEC on APL visitor and VIP tours
  - Support referrals for demonstrations from NIAEC stakeholders
- Synthesize visitor feedback to influence IA research prioritization and investment
- Support NIAEC customers seeking to transition demonstrated technologies to their programs, systems, exercises, or demonstrations

NIAEC

NIAEC Administration

NIAEC is administered through the cooperation of multiple organizations with vested interests in seeing IA technologies effectively and appropriately transitioned to operations

NIAEC

Current NIAEC Status

- Inaugural demonstration complete – facility open for visitors
  - Visitors thus far include: JTF-GNO, PACFLT, ACERT, 1st IOC, J6, GIAP, DIAP
- NIAEC demonstration and outreach at the IA Workshop
- NIAEC-hosted technology demonstrations at REBL Symposium
- System and technology selection for next demonstration is on-going
  - Highlighting IA Best Practices and the impact on attacker success and mission objectives
  - Coordinating with IA representatives across the community

NIAEC


NIAEC
NATIONAL INFORMATION ASSURANCE
ENGAGEMENT CENTER

The Next NIAEC Demonstration

Integrating IA Best Practices into Operations

Best Practices Challenge

- Most IA Leaders claim *'If we could only get the operators to follow best practices we could dramatically reduce our risk'*

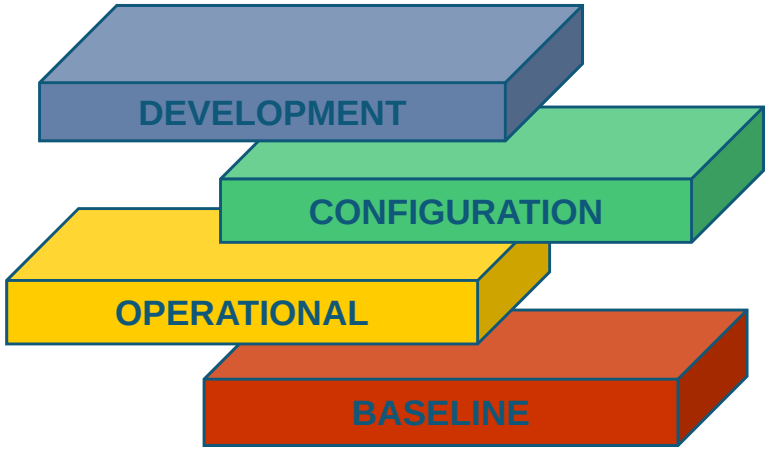
What are *the* IA Best Practices?

Which practices are most important to convey to operational community?

How would we convey the practice – what attack or vulnerability will highlight them?

What systems or platforms will we need to have in place to showcase?

Are there tools, platforms, solutions that could further enhance the best practice?



NIAEC

Best Practices Approach

- **Select a Top X list of Best practices**
  - What gets our operators the most bang for the buck
  - What can we do today with little or no investment to improve
  - Recommend things that also allow us to head down a path for further improvement
- **Span categories of risk type and best practices types**
  - User-based versus enterprise-base
  - Configuration practices versus operational execution
- **Apply over a compelling OPSIT that allows us to highlight the benefits of best practices**
- **Showcase:**
  - Mature, certified solutions or tools
  - Emerging operational configurations, standards, or mandates (DoD FDCC)

NIAEC

NIAEC Selection Phase

NIAEC Demonstration Components

- *Mission-Focused*
- Scenario: OPSIT/operational events depicted
- System: Environment that 'hosts' the scenario – what operational system(s) are used to achieve the mission
- *IA-Focused*
- Attack Plan: Threats/challenges showcased and how they will be implemented
- Technology: The IA component or configuration that is being applied against the threats

NIAEC

Current Activities

- OPSIT Selection and Definition
  - Targeting a NIPRnet-based scenario that highlights aggregate threats and a longer time-span
  - Candidates include TRANSCOM, local and federal first-responder coordination, etc.
- Best Practices Selection
  - Key organizations participating include NSA Red Team and Blue Team, J6, JTF-GNO, DIAP IA Best Practices WG, DISA
  - Actively seeking additional input
- Enabling Technology Integration
  - Selecting candidate IA solutions or enabling technologies that would enhance operator abilities to follow best practices
  - Seeking to identify candidate solutions for this or a future demonstration

NIAEC

Summary

- NIAEC represents a community-wide resource available to define and characterize IA threats and pair operational need with emerging solutions
- NIAEC demonstrations are appropriate for operational, acquisition, and policy-making community representatives
- Development activities, service laboratories, and agencies are excellent sources of technologies and scenarios for demonstration

We welcome all inquiries and encourage you to schedule a visit to a NIAEC demonstration

niaec@jhuapl.edu

NIAEC

Acronyms

ACERT	*Army Computer Emergency Response Team*
CONOPS	*Concept of Operations*
DIAP	*Defense-wide Information Assurance Program*
DISA	*Defense Information Systems Agency*
FDCC	*Federal Desktop Core Configuration*
GIAP	*GIG Information Assurance Portfolio*
GIG	*Global Information Grid*
IA	*Information Assurance*
JHU/APL	*The Johns Hopkins University Applied Physics Laboratory*
JTF-GNO	*Joint Task Force-Global Network Operations*
NIAEC	*National Information Assurance Engagement Center*
NSA	*National Security Agency*
OPSIT	*Operational Situation*
OSD/NII	*Office of Secretary of Defense/Network & Information Integration*
PACFLT	*Pacific Fleet*
REBL	*Red Team/Blue Team Symposium*

NIAEC