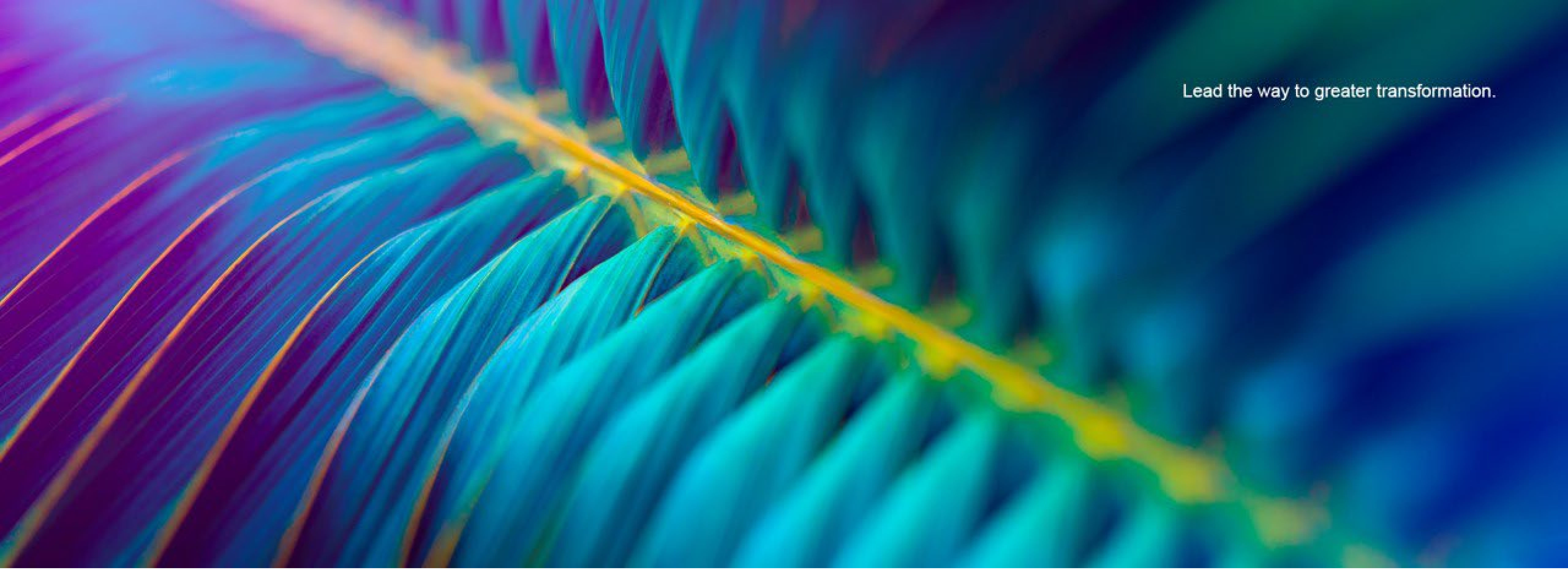


GDIT Zero Trust in DDIL Environments

Garrett Yee, MG USA (Retired)

GDIT Army and Defense Agencies VP/General Manager

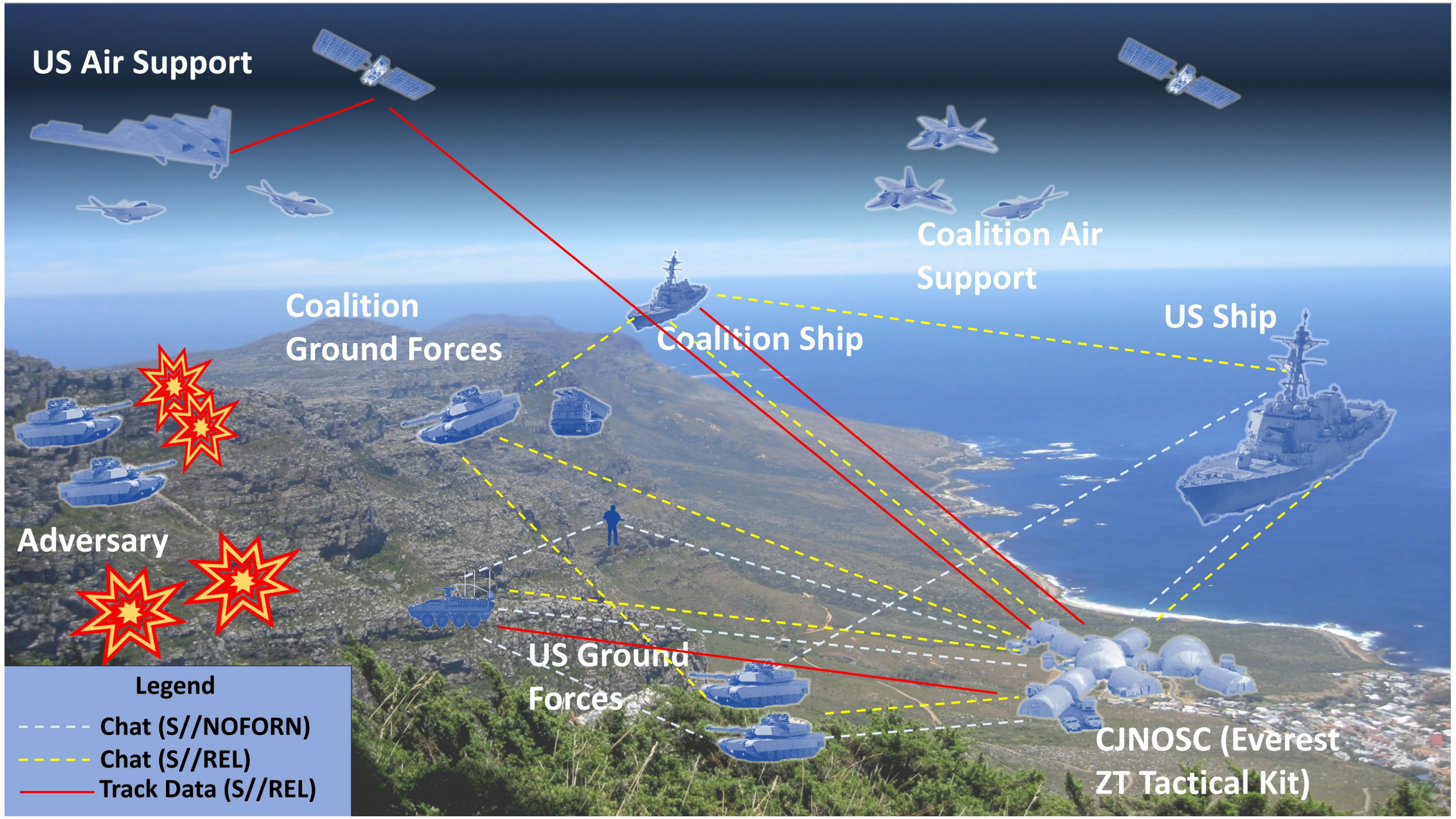
GENERAL DYNAMICS
Information Technology

Art of the Possible.

I Corps ZTA Operating Environment: Tactical/D-DIL CJADC2

Background

- GDIT Supported I Corps creating a Tactical Zero Trust capability in a multilateral Mission Partner environment during Exercise Talisman Sabre 23, and Yama Sakura 85 leveraging existing Army I Corps infrastructure
- GDIT Implemented improved Zero Trust capability maturity, aligned with the DOD CIO Zero Trust "Fan Chart"
- Tactical Edge ability to support ad hoc data sharing in D-DIL environment and federation with enterprise services
- The ZTA MPE capabilities included Federation of policies and data with coalition and joint mission partners



Zero Trust in DDIL Environments – Lessons Learned

Mission Drives Zero Trust Architecture use cases.

- Zero Trust Architecture works best when it is enabling something – ie Mission.
- Mission focused use cases help define how ZTA is a help and not an hinderance.

Start with available technology and then add new capability.

- Are there existing capabilities that are already available that can be used as a baseline?
- Can those capabilities be integrated to support ZTA?
- What capabilities need to be added to support ZTA for the set of Mission-driven use cases?

Synchronization Happens, plan for it.

- Once communications are available what information is shared between enclaves?
- How are conflicts resolved between enclaves?
- How much bandwidth is available to share information?
    - **Zero Trust is important – but mission comes first!!!**

© 2024 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Lessons Learned from TS23 and YS85

Use Cases are critical!

- Use cases make ZTA real and not just a fan chart- the goal became capability, not compliance.
- Having ZTA use cases defined with I Corps and supporting organizations provided concrete, testable objectives for ZTA.

When implemented correctly, ZTA is a help not a hinderance

- Complexity was reduced in the I Corps Mission Partner Environment by simplifying Authentication and Authorization for collaboration tools while enhancing the resiliency of the system
- ZTA harmonizes Computer Network Defense Teams efforts with Server Teams by focused feedback of user/device behavior into risk-based authentication/authorization

Incrementally Implement Capability

- Disruptions were limited – incremental implementation minimized risk
- Adjustments for future efforts were introduced based on Warfighter feedback

© 2024 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Yama Sakura 85

© 2024 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.